Symantec
A Division of Broadcom

產品型錄

Messaging Gateway

具有進階威脅與資料防護功能的郵件安全閘道

簡介

電子郵件是公務及業務最常使用的正式溝通工具，自然成為駭客覬覦的第一大目標。 電子郵件安全解決方案的廣泛採用，也迫使攻擊者尋求更精密的戰術來滲透組織。在與駭客攻防的競賽中，傳統的基本攔截工具早已無法保護組織免受目標式的勒索軟體、魚叉式網路釣魚、商務電子郵件入侵(BEC)和其他複雜的電子郵件攻擊。 組織必須與時俱進採用最新的防禦技術（例如機器學習、URLs鏈接隔離以及具有有效沙箱和檔案引爆的行為分析）的多層式方法來增強傳統電子郵件安全技術的不足。

訊息安全解決方案

針對內部部署郵件環境，賽門鐵克提供必要的雙向：入埠(inbound)及離埠(outbound)強大的進階威脅防護與防垃圾郵件解決方案，可保護您的電子郵件免受勒索軟體、魚叉式網路釣魚以及商務電子郵件入侵(BEC)等狡詐的電子郵件威脅。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。

Messaging Gateway 郵件安全閘道，結合多層式防護技術，可有效偵測、封鎖以及隔離可疑的檔案：

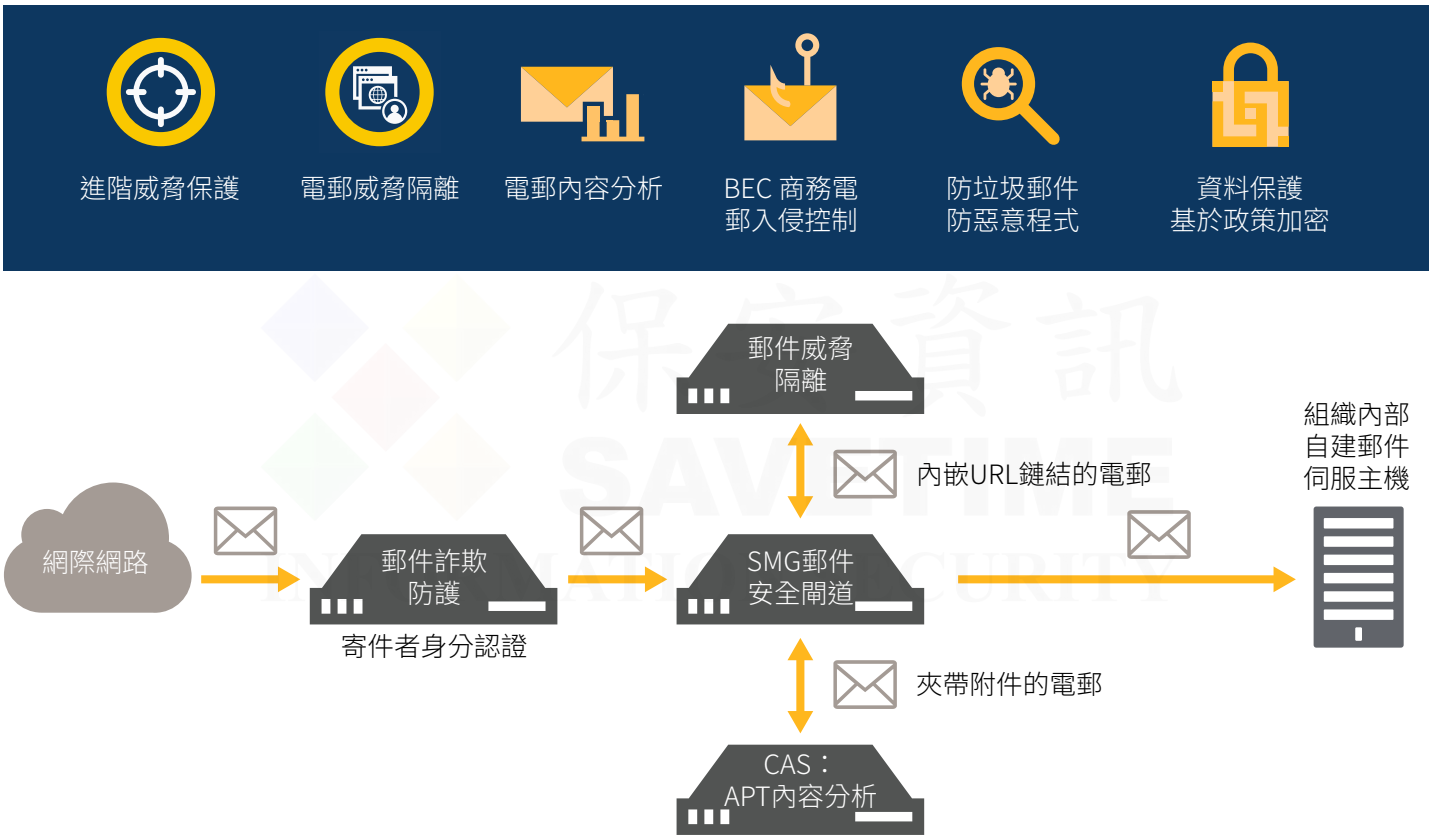
- 使用進階啟發學習法、BEC 詐騙分析、強制執行寄件人身分驗證 (DMARC、DKIM 與 SPF)，以及網域情報等功能，協助攔截誤植網域名稱並識別詐騙。
- 結合賽門鐵克全球與本地寄件者信譽資料庫和客戶專屬垃圾郵件規則，對垃圾郵件以及電子郵件地址搜尋攻擊(Directory Harvest Attack，簡稱DHA)加以封鎖，攔截多達 90% 的不當電子郵件，使這些郵件無法進入您的網路。
- 進階內容過濾控制可避免諸如電子報和行銷電子郵件等不當電子郵件進入使用者的收件匣。
- 利用以賽門鐵克全球資料庫為基礎的網址信譽過濾技術，抵禦魚叉式網路釣魚活動中使用的電子郵件內的惡意連結， 包含進階網路釣魚變體偵測技術，探查與已知網路釣魚攻擊類似的網路釣魚連結，藉以防範惡意連結。
- 移除 Microsoft Office® 和 PDF 附件中的零時差文件威脅及停用URL連結，保護使用者免於勒索軟體之類的目標式攻擊。Messaging Gateway通過把每一個郵件附件替換成數字式的無害副本，從而從根源上阻止了收件人與惡意程序的接觸。這項產業界獨家技術能夠詳細檢查所有帶有Microsoft Office 和 Adobe PDF附件的電子郵件，並建立附件的重構版本，在郵件和新附件發送給收件人之前，刪除任何可被利用的活動內容，例如Javascript和嵌入式Flash。

SMG郵件安全閘道可同時整合：Symantec™ Content Analysis (APT內容分析)、Symantec Email Threat Isolation (郵件威脅隔離)以及 Symantec Fraud Protection(郵件詐騙防護)，提供更進階的威脅防護、威脅分析以及冒充防禦功能，能使組織快速回應目標攻擊及進階攻擊。

這樣的防護能力是由全球規模最大的民間威脅情報網路:賽門鐵克全球威脅情報網路 (GIN：Global Intelligence Network)所提供的全球洞察力為後援，可提供深入威脅態勢的全方位能見度，利用來自 157 個國家、1 億 7,500萬個端點、8,000 萬個 Web Proxy 使用者及 5,700 萬個攻擊偵測器的遙測資料，帶來更優異的安全成效。

郵件安全閘道
APT進階威脅掃描平台
郵件威脅隔離
郵件詐騙保護

*2018年 5月開始提供



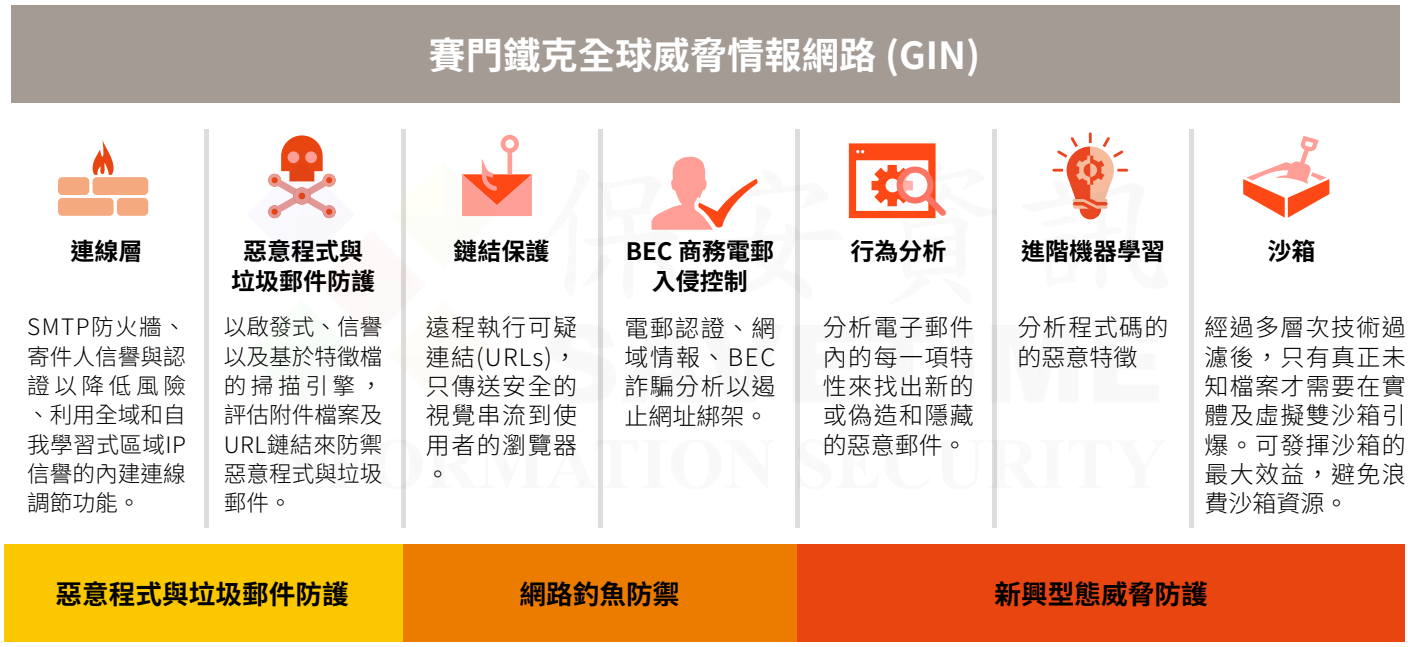
圖示：賽門鐵克郵件安全閘道(SMG)、郵件詐欺防護、CAS：APT內容分析與沙箱 以及郵件威脅隔離的完美整合。

利用進階威脅防護技術，藉以防範惡意連結與惡意檔案

電子郵件威脅隔離可對魚叉式網路釣魚和針對目標式攻擊活動中使用的惡意連結提供進階保護，該功能可遠程執行可疑連結(URLs)。 該技術只傳送安全的視覺串流到使用者的瀏覽器，因此能協助免除源於網頁的威脅，讓這類威脅不會感染使用者的裝置。電子郵件威脅隔離還可以將使用者設定為唯讀模式，因此能避免使用者不慎提交企業憑證及其他敏感資料到這些網站。

內容分析(Content Analysis)透過機器學習、預測性檔案分析以及虛擬機器感知沙箱等多種進階技術，自動升級及代理零時差威脅，揭示惡意行為並安全引爆可疑檔案，抑制如勒索軟體等最新的檔案式攻擊：

- 使用精密的預測性檔案分析和機器學習對結果進行分類並根據在沙箱揭露的結果，採取正確的回應－捨棄、傳遞或傳遞檔案以進行行為分析。
- 提供可自定義的虛擬機(virtual machine)或基於模擬(emulation-based)的沙箱，以複製實際運行環境，以準確分析和偵測具有迴避虛擬機感知的惡意檔案。



圖示：賽門鐵克郵件安全閘道(SMG)的多層式威脅偵測技術。

借助威脅分析，加速您對目標式攻擊的回應

針對網路上複雜攻擊活動進行深入分析，阻止目標式進階威脅傳播。 這包括入侵指標(IOC)，例如檔案雜湊、檔案結構、威脅風險評分以及所使用的攻擊技術。 安全分析師可以使用本機儀表板或透過與第三方SIEM關聯進階威脅資訊的整合。SMG整合CAS所提供的內容分析提供以下威脅情報，以幫助加速您對威脅調查和目標式攻擊的回應：

- CAS的內容分析提供惡意軟體揭露報告，該報告提供可採取行動的情報，例如關鍵的惡意指標、詳細的靜態和動態事件活動，可供下載的跡象和資源分析以及生成的威脅風險分數。
- SMG的儀表板摘要和詳細報告讓你對威脅趨勢、攻擊統計資料和潛在的法規遵循問題一目瞭然。 自動即時可提供有關病毒爆發、違反策略和電子郵件隔離資訊等通知。
- 運用由SMG交由CAS的系統日誌，使用第三方 SIEM 關聯進階威脅資訊，發現攻擊趨勢並識別出目標式攻擊的收件者。
- 透過與 Symantec Endpoint Protection 和 Symantec ProxySG 的整合，可以跨網路、端點和郵件通道加速威脅分析、攔截與矯正。

防止資料外洩 (DLP)

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：

- 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郵件內文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。超過100個預先建立的字典、樣式、政策範本，協助您輕鬆實施自動化資料保護與強制執行政策。
- 對郵件通道強制執行 TLS 加密：透過對來自特定網域的入／出埠郵件強制執行 TLS 加密的選項，可使與信任夥伴和寄件者的通訊更加安全。
- 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 (DLP)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。

"賽門鐵克在 2018 年 10 月的 Radicati 安全電子郵件閘道市場象限 (Radicati Secure Email Gateway Market Quadrant) 報告中獲選為領導者。"

"在「2019 年第二季 The Forrester Wave™：Enterprise Email Security」報告中，將賽門鐵克評選為領導者。"

若要進一步瞭解 郵件安全閘道

若要進一步瞭解 APT內容分析及沙箱

若要進一步瞭解 郵件威脅隔離

若要進一步瞭解 郵件詐騙防護

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)

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

19D214219_DS_On-Premises_Email_Security_with_ATP_EN