賽門鐵克電子郵件安全在競爭中脫穎而出

電子郵件是迄今攻擊者傳播惡意軟體和入侵組織最普遍的方法，因為電子郵件的無遠弗屆、低成本以及易於假冒的特性，使電子郵件攻擊對網路犯罪分子有利可圖。這些攻擊已經從傳統的亂槍打鳥發送鋪天蓋地的垃圾郵件和網路釣魚電子郵件，不斷演變為全新、複雜的電子郵件威脅，例如：勒索軟體、魚叉式網路釣魚、商務電子郵件入侵 (BEC) 詐騙……等，槍槍斃命的鎖定目標式攻擊。

這些攻擊經常是有針對性，使用社交工程來欺騙資安認知脆弱的用戶下載惡意軟體、點擊可疑的鏈結或上當受騙的電子郵件。他們還利用複雜的煙霧彈技巧來躲避偵測，例如：將惡意軟體隱藏在看起來無害的檔案中、混淆惡意連結或對電子郵件域進行域名仿冒。

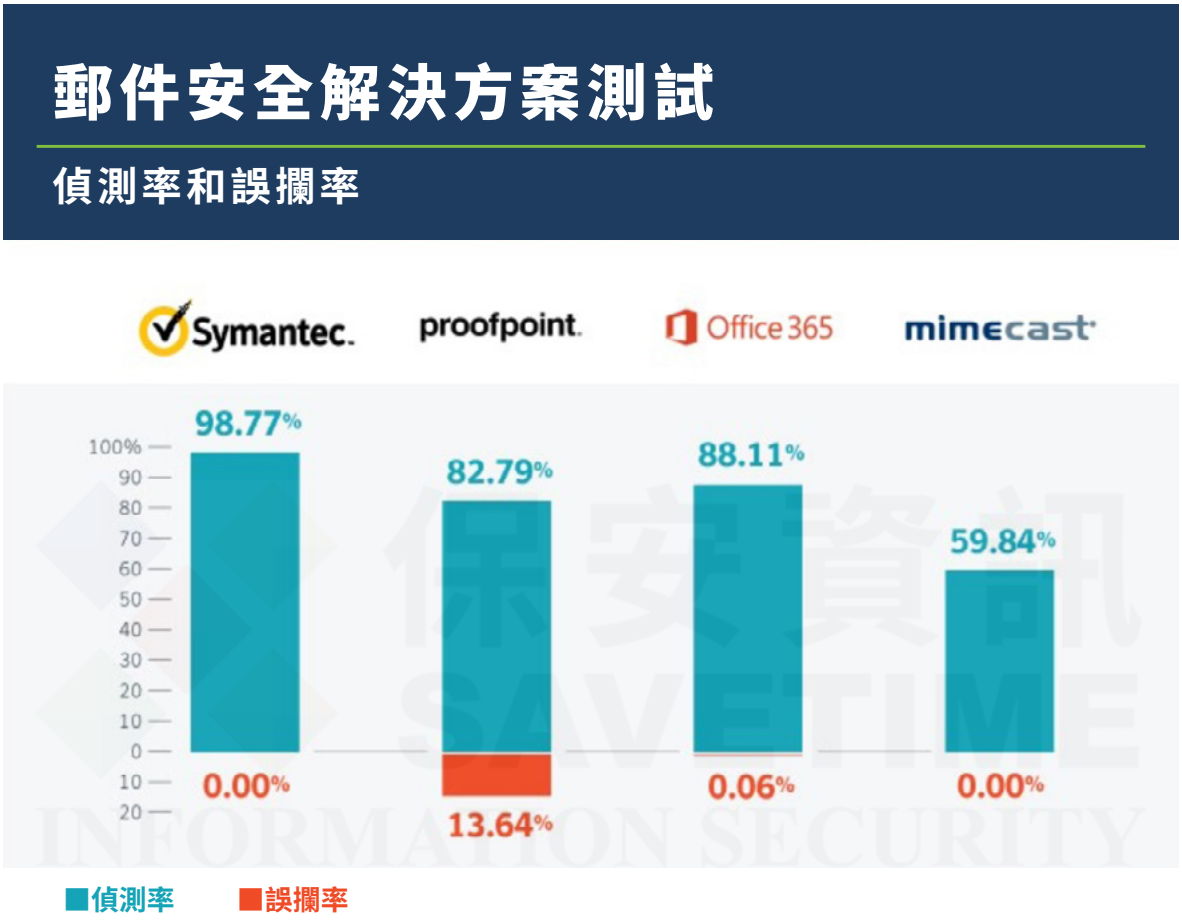
隨著電子郵件威脅變得日益先進，企業需要一個能有效且精確地阻擋新又複雜的電子郵件攻擊解決方案。賽門鐵克郵件安全雲端服務：Symantec Email Security.cloud 是一項全方位的雲端服務，能夠防護您的電子郵件，同時強化雲端內建生產力工具 (Office 365 和 G_Suite) 的安全性。它可利用多層式偵測技術和來自全球規模最大的民間威脅情報網路的洞察力，高效率且精準地阻擋全新的複雜電子郵件威脅，像是魚叉式網路釣魚攻擊、勒索軟體和企業電子郵件入侵。包括抵禦魚叉式網路釣魚的最佳防護，這是由於 Symantec Email Security.cloud 會在傳送電子郵件前即時追蹤並評估惡意連結，避免威脅嘗試使用煙霧彈技巧來躲避偵測。

賽門鐵克與競爭對手的比較

在賽門鐵克，我們努力不斷創新，提高解決方案的功效和準確性。這包括測試評估我們的解決方案與其他供應商的產品，有助於我們不斷鞭策自己，為客戶提供創新的進步發展。因此最近進行一項內部測試，以衡量我們電子郵件安全雲端服務的威脅檢測能力，與其他同業解決方案的比較。

我們將「賽門鐵克郵件安全雲端服務」與 Proofpoint、Microsoft 和 Mimecast 電子郵件安全解決方案進行測試。在這項測試中，總共發送 1900 封電子郵件，其中包括惡意軟體、網路釣魚、垃圾郵件、大宗郵件和乾淨的電子郵件組合，在 15-25 天的時間內，發送到每個電子郵件安全解決方案。這次測試中，我們保持 12:1 的乾淨（其中包括大宗郵件）與不良（惡意軟體＋垃圾郵件）郵件的比例。

結果（見圖1）顯示，賽門鐵克在電子郵件威脅檢測的有效性和準確性方面，仍然處於領先地位。在所有測試的解決方案中，賽門鐵克電子郵件安全雲服務具有最高的有效性（檢測到98.77% 攔截率）和準確性（0.00%的誤報率）。



為什麼賽門鐵克會脫穎而出？

我們所測試的許多解決方案都使用標準技術，例如：防毒軟體特徵檔比對、域名黑名單以及信譽分析，來阻止電子郵件威脅。相較之下，賽門鐵克採取一系列獨特的電子郵件安全方法，像是進階啟發式偵測技術、即時連結追蹤和模擬控制、來自全球規模最大的民間威脅情報網路的洞察力，找出目標式攻擊並保護電子郵件免於威脅、使用者錯誤和資料外洩。

首先，電子郵件安全雲端服務利用進階啟發式偵測技術，可封鎖能夠迴避傳統安全解決方案偵測的勒索軟體、目標式攻擊和最新的新興威脅。這些預測性的啟發式技術會利用電子郵件內的每一項特性，找出新的或偽造的攻擊，特性包括有傳送行為、訊息內容、附件和社交工程技術。其中也包含深層的程式碼分析，判斷電子郵件內是否包含任何惡意程式碼的元件，以防攻擊者將程式碼重複使用在全新的攻擊上，藉此封鎖勒索軟體的最新變種。此外，這些功能還

可利用檔案分解來偵測隱藏在附件中的惡意軟體，遏止使用規避技術的隱匿惡意程式等威脅。例如：此功能可識別將惡意程序檔隱藏在文件內的勒索軟體，即使文件是藏在 zip、Office 文件、PDF……等其他檔案內。

接下來，賽門鐵克郵件安全雲端服務使用全面的即時連結追蹤 (Real-Time Link Following) 技術，以提供最強大的保護，防止魚叉式網路釣魚連結。大多數供應商依靠反應式黑名單或簽名來阻止魚叉式網路釣魚連結，而賽門鐵克則不同，它在電子郵件傳送之前，就已經即時追蹤並評估可疑的連結。這一點非常重要，因為許多魚叉式網路釣魚攻擊 (包含全新的鏈接)，反應式黑名單或簽名技術通常會錯過。有些解決方案會跟蹤重定向鏈接的一或兩個跳躍點，而不是全面。而賽門鐵克郵件安全雲端服務會跟蹤鏈接，透過多個跳躍點到達其最終目的地，即使使用短網址 URL 或基於時間的延遲等規避技術。此外，不管鏈接經過幾次的重定向，其最終目的發現任何檔都會被下載，並由我們先進的啟發式方法進行掃描，以確定它們是否是為惡意，還能即時分析網站內容，並防止具有威脅連結的電子郵件出現在使用者收件匣中。

最後，賽門鐵克透過賽門鐵克全球情報網的洞察力，來識別最隱蔽和最持久的威脅，賽門鐵克全球威脅情報網路 (GIN：Global Intelligence Network) 是世界上最大的民間威脅情報網路，GIN 所提供的全球洞察力為後援，可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，透過收集和分析大量的情報，帶來更優異的安全成效。

推動客戶和行業創新貢獻心力

當這些能力結合在一起時，就形成業內最有效和最準確的電子郵件安全解決方案。我們一直希望透過競爭性測試來改進這個解決方案，這有助於加強和提高我們的解決方案，以保持對最新威脅的領先，繼續成為客戶值得信賴的網路安全合作夥伴。

有關賽門鐵克郵件安全雲端服務更多資訊，歡迎與 **保安資訊** 連繫
要更詳細瞭解，請訪問 **賽門鐵克郵件安全雲端服務最新資訊**

原廠網址：https://community.broadcom.com/symantecenterprise/viewdocument/how-does-symantec-email-security-st?CommunityKey=6d211047-d256-4113-b98b-e4ef0d6510c7&tab=librarydocuments
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。