輕鬆解決日益複雜的郵件安全問題
--Symantec 郵件安全解決方案擴增及強化功能介紹

根據統計招致企業感染病毒等惡意程式(會衍生更嚴重的資安損害)的主要來源為：電子郵件、網頁瀏覽以及隨身碟之類的行動儲存媒體(佔98%的約有50幾種)，其中電子郵件約佔了整體的70%以上，攻擊者很容易透過社交工程的手法，誘導受害者開啟惡意的附件及連結， 特別是現在的攻擊者多為商業型營利的駭客組織或國家級資助的專業網軍，所以使用傳統的防護機制，往往看似風平浪靜，但只要一出事，總是迅雷不及掩耳般地造成山崩地裂的大災難。其實是針對性的攻擊，在埋伏一段時間後，只要時機成熟，就可以在很短的時間，遍地開花，讓企業瞬間束手無策舉白旗。

今天要向大家介紹的賽門鐵克郵件安全解決方案總共有三種：第一：Microsoft Exchange Server 防護(SMSMSE：Symantec Mail Security for Microsoft Exchange Server)、第二：安全郵件閘道(SMG：Symantec Messaging Gateway)以及第三：郵件安全雲端服務(Email Security.Cloud Service)。

第一種：**SMSMSE**是安裝在Microsoft Exchange Server 本機上的防護軟體，它是屬於應用程式層級的防護，有別於作業系統層級的防護(像SEP 就是)，所謂應用程式層級就是它能與Exchange 完美協同運作，能看得懂Exchange 郵箱的內容，有辦法快速精準判斷是否安全或不正常。

第二種：**SMG**--安全郵件閘道，基本上它就是一台快速的、專用於郵件安全檢查或內容過濾的郵件遞交伺服主機(同時支援實體與虛擬環境)，能在您的Exchange 或其他自建或雲端郵件主機收信之前先行過濾(內送)，也可以在寄出之前幫忙檢查是否(外寄)郵件違反安全政策。SMG原生的DNA強項就是採用BrightMail 的專利技術，輕鬆就能達到：垃圾郵件的偵測率高達99%，而誤攔率低於百萬分之一，而被最多ISP廠商選為過濾垃圾郵件的合作對象。而Symantec的惡意程式及進階威脅(APT)的防禦能力，更是業界翹楚。特別是Symantec 併購許多特定安全領域的龍頭公司，像是PGP加密、BlueCoat 網頁安全代理及分類/過濾、FireGlass 是作安全遠端瀏覽的威脅隔離技術的，Norman 的沙箱及多重掃描引擎…，這些最佳的安全功能，都可以與SMG 作緊密的整合。

第三種：郵件安全**雲端服務**(Email Security.Cloud Service)，它比微軟O365 及谷歌G Suite 所提供的郵件安全防護更強大，可以做為O365及G Suite的安全強或安全替代方案，您也可以它視為SMG的雲端版郵件安全服務，它有SMG 所有的基本功能及加值功能，另外拜雲端運算能力以及擴充延展性的優勢，它有幾項SMG無法達到或帳號數目不多/不具經濟規模只能望梅止渴的自建型尖端功能：

- **即時連結追蹤技術(賽門鐵克郵件安全雲端服務的標準防護功能之一)：**即時連結追蹤可在傳送電子郵件前，封鎖魚叉式網路釣魚攻擊、目標型攻擊和其他進階威脅所使用的惡意連結。與利用特徵檔來封鎖魚叉式網路釣魚攻擊的郵件安全解決方案不同，賽門鐵克搶在使用者點選時即深入評估可疑連結，更可以主動遏止全新及已知的網路釣魚攻擊，深入評估並追蹤至最終目

的地，即便攻擊者嘗試使用如多個重新導向、短網址，被挾持的網址或時間延遲等規避技巧，能夠輕鬆躲避傳統安全解決方案的偵測，卻難逃賽門鐵克的天羅地網。下載在目的地網址找到的任何內容，並且執行深入啟發式分析，以判斷連結是否為惡意程式。URL點擊時防護和即時連結追蹤為深入的鏈接評估提供強大的支持，能夠提供最有效的電子郵件保護，以抵禦魚叉式網路釣魚、目標式攻擊以及包含惡意鏈接的其他進階威脅。

- **URL 點擊時防護(Click-time URL Protection)：**分析用戶點擊網頁鏈接，封鎖電子郵件傳送後透過觸發連結發動的魚叉式網路釣魚、目標式與進階攻擊，此項功能被包含於ETDR。
- **資訊安全認知培訓：**ETDR 包括資訊安全認知培訓的線上內容與評估工具，可以經由評估使用者對網路釣魚威脅的準備程度來降低網路釣魚的風險，同時識別和培訓組織中最易受攻擊的使用者以進行網路釣魚攻擊。可自定的安全評估使您可以通過模擬整個組織中最新的真正的網路釣魚威脅來評估使用者對網路釣魚攻擊的準備度。模擬攻擊後，詳細的報告和管理儀表板可幫助您對員工的準備度的基準作測試，並找出最容易受到攻擊的用戶。最後，您可以通過使用培訓通知來教育使用者有關目前與新興的網路釣魚攻擊，並執行重複評估以跟踪用戶的準備情況，從而提高用戶對網路釣魚威脅的準備程度，隨著時間過去，讓強固的資訊安全認知成為自然形成的企業文化。此項功能被包含於ETDR。
- **賽門鐵克電子郵件威脅偵測與回應(ETDR)：**利用進階電子郵件安全分析，提供目標式攻擊最深入的能見度，加快對目標式與進階攻擊的應變速度。這些情報包括對惡意和乾淨電子郵件的洞察力，以及對網址、檔案雜湊和目標式攻擊資訊等超過60個資料點獲得比其他廠商更多的入侵指標(IOC)。如果您已理解EDR(端點偵測與回應)的運作原理及效益(EDR透過專利的雲端沙箱及大數據的交叉比對、關聯分析的類SIEM機制，可以比先進的端點防護軟體，具備更高的偵測力，更可以及早發現及掌控企業內部更完整的安全態勢，即使事有蹊蹺，也能幫忙安全人員快速追根究底，掌握資安事件的來龍去脈，輕鬆就能讓整起事件水落石出)，那麼您就把這個情境轉移到郵件，就是這樣簡單，這是專為Email Security.Cloud Service 所提供的加值服務。
- **內容過濾與雲端沙箱：**這個功能SMG 也能選購CAS專用主機及雲端服務。CAS 就是利用雙重掃描引擎及其他行為分析以及檔案信譽等多重偵測技術，最大化已知及未知惡意程式的過濾(以節省後續沙箱的資源並加快處理速度)，然後再將須要遞交至沙箱引爆的可疑檔案同時遞交給實體主機及虛擬環境這兩種沙箱，這是Symantec領先業界的技術，特別是針對俱虛擬感知能力的惡意程式特別有效。
- **電子郵件威脅隔離：**這個功能SMG 也能選購。這個功能其實就是Web Isolation 在電子郵件的使用實例，在雲端或地端自建一個讓網頁瀏覽或檔案下載的一次性安全容器的真實執行環境，然後把執行的結果傳回本機電腦，任何有害的連結或檔案，完全不會落地，保證100%安全。

上述只是主要功能的大致說明，建議參考以下的型錄連結，獲得更詳盡的資訊，如有業務及技術諮詢，歡迎來電洽詢，保安資訊將竭誠為您服務。

- **賽門鐵克郵件安全雲端服務中文型錄：** Symantec Email Security.cloud Service
- **賽門鐵克電子郵件威脅偵測與回應中文型錄：**ETDR：Symantec Email Threat Detection and Response
- **賽門鐵克網頁威脅隔離中文型錄：**Symantec Web Isolation
- **賽門鐵克安全郵件閘道中文型錄：**SMG：Symantec Messaging Gateway
- **賽門鐵克內容分析與惡意程式分析(沙箱)中文型錄：**CAS：Content Analysis System
- **賽門鐵克Microsoft Exchange Server防護中文型錄：**SMSMSE：Symantec Mail Security for Microsoft Exchange Server

Symantec在端點、電子郵件以及網頁防護，皆有最完整的防護機制，同時也能在這三個控制點，透過AI為後盾的關聯分析與情資交叉比對的協同運作，能在第一時間就發現目標式攻擊，更能發現入侵後的初期入侵跡象、中期橫向移動以及後期的資料外洩及更大的危害，都能有效偵測。在2019/11，博通併購賽門鐵克後，更加重投入資源在RD上，同時也大大降低交易複雜性，將料號精簡為功能多合一、實體與虛擬、地端與雲端等符合全功能多情境--並以極具競爭力的價格來提供，讓顧客更喜歡、更容易使用/採購賽門鐵克。

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有IT Team的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入Symantec解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊：
  保安資訊有限公司
  http://www.savetime.com.tw
  0800-381500、0936-285588