Symantec by Broadcom

解決方案簡介

Email Security.cloud service

簡稱Symantec ESS，賽門鐵克郵件安全雲端服務

因應現代網路威脅環境所需的全面且完整的電子郵件安全解決方案

快速一覽

Email Symantec Security.cloud service --簡稱 Symantec ESS，賽門鐵克郵件安全雲端服務，提供一種全面的解決方案，可保護地端自件郵件系統以及雲端郵件服務平台的保護

主要效益

- 增強對各種網路進階威脅 (APT) 的保護
- 提升營運績效
- 效能卓越成本效益高的郵件安全解決方案
- 滿足日益嚴峻的法規遵循性、資料隱私要求
- 提高使用者資安意識

主要功能

- 頂尖的檢測和預防能力
- 威脅隔離能力
- 全面的威脅情報
- 整合使用者的資安教育和認知分析
- 與資安生態系統的緊密整合

概觀

電子郵件仍然是網路攻擊的主要目標，網路犯罪分子利用它傳播，諸如勒索軟體、商業電子郵件詐騙 (BEC) 和網路釣魚等威脅。根據 2024 年 Verizon 資料外洩調查報告，電子郵件是散佈勒索軟體的主要途徑，也是資料外洩事件中第二常見的傳播途徑。IBM 發佈的《2023 年數據洩露成本報告》也揭示電子郵件攻擊的驚人成本，BEC 平均為 467 萬美元、網路釣魚為 476 萬美元、社交工程攻擊為 455 萬美元。

攻擊者更頻繁地採用老練的手法，例如：魚叉式網路釣魚、網域詐騙和混淆式網址連結，繞過傳統的電子郵件防禦。遷移到雲端服務之電子郵件系統 (例如：Microsoft Office 365 和 Google Workspace) 企業面臨更高的脆弱性，因為內置安全性往往無法滿足需求。傳統電子郵件安全解決方案受限於分析不足和整合操作上的隔閡，難以滿足當今複雜威脅環境的要求。這造成資安防護的缺口、營運上的複雜挑戰，以及資料洩露、未能滿足安全合規性和財務損失的風險上升。穩健且整合性高的郵件安全解決方案現在已成為必需。

賽門鐵克郵件安全雲端服務 (Symantec® Email Security.cloud Service：ESS) 簡介

賽門鐵克 ESS 提供全面的郵件安全解決方案，可同時保護雲端服務的電子郵件系統 (Office 365、Google Workspace) 和地端自件郵件系統 (Microsoft Exchange、Linux-Based 的專用郵件主機硬體裝置)。賽門鐵克 ESS 的多層次防禦技術能夠阻止進階威脅，例如：勒索軟體、魚叉式網路釣魚和商業電子郵件詐騙 (BEC)，同時得力於先進的分析和與賽門鐵克全球情報網路 (Symantec Global Intelligence Network : GIN) 的整合，能增強對攻擊活動的可見性。

圖 1：業界最全面完整的郵件安全保護

這個全面電子郵件安全解決方案提供端對端的保護，從預防、隔離到回應。它還著重使用者準備度、架構配合性和相容性，以縝密整合組織內的其他安全架構並最大化投資回報。

預防：第一道防線

預防是電子郵件安全的基石。Symantec ESS 增強電子郵件系統的原生安全性限制，有效地防止惡意軟體和電子郵件威脅，同時將誤報降到最低。先進的檢測技術和來自賽門鐵克全球情報網路 (Symantec Global Intelligence Network：GIN) 之遙測能夠阻止複雜的攻擊，例如：勒索軟體、魚叉式網路釣魚和商業電子郵件詐騙 (BEC)。透過過濾垃圾郵件和不需要的電子郵件，例如電子報和廣告信，Symantec ESS 在保持強大保護的同時提升用戶之生產力。在面對潛在的問題或風險時，採取預防措施是最佳的應對方式，可以避免問題發生或降低其嚴重程度。

惡意軟體和垃圾郵件防護

- 惡意軟體和垃圾郵件防禦：利用信譽分析、防毒引擎和反垃圾郵件簽名特徵檢查連結和附件，有效阻止垃圾郵件和惡意軟體。
- 連線 (IP) 層級保護：透過流量限縮和丟棄異常的 SMTP 連線來降低垃圾郵件和惡意軟體的風險。
- 威脅隔離：透過隔離可疑的電子郵件附件，防止勒索軟體和其他惡意軟體感染使用者。這項技術還會隔離承載惡意軟體的風險或未知電子郵件連結，保護使用者和設備免受感染下載的威脅。

網路釣魚防禦

- 連結保護：在電子郵件傳遞前即時掃描連結，並在點擊時再次掃描，將其追蹤到最終目的地—即使攻擊者使用先進的規避技術。先進的網路釣魚變種檢測能夠識別並阻止與已知網路釣魚攻擊相似的連結。
- 冒充控制：透過此用精密的冒充引擎提供強有力的保護，阻止模仿合法用戶或網域的威脅，以防止商業電子郵件詐騙 (BEC) 和欺騙。
- 威脅隔離：以唯讀模式開啟有風險或未知的網站連結，保護使用者免受網路釣魚攻擊。

Symantec ESS 是最有效又準確的電子郵件安全解決方案，利用多層式偵測技術，像是進階啟發式偵測技術、即時連結追蹤和模擬控制來阻擋全新的複雜電子郵件威脅，例如：魚叉式網路釣魚攻擊、勒索軟體和企業電子郵件入侵。這樣的防護能力是由全球規模最大民間威脅情報網路所提供的洞察力為後援，可提供深入威脅態勢的全方位能見度，每天利用來自 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和主動防禦策略。

隔離：通過新興威脅檢測增強預防

Symantec ETDRI--賽門鐵克電子郵件威脅偵測、回應與隔離 (ETDRI：Email Threat Detection Response and Isolation) 是一項雲端服務，透過結合先進技術，擴展 Symantec 電子郵件安全的能力，以在電子郵件攻擊對使用者或系統造成傷害之前化解這些攻擊。

重要功能

- 雲端沙箱：透過我們的雲端沙箱環境發現複雜和進階的攻擊。該服務採用技術類比人類行為，並在虛擬和實體硬體上執行可疑檔，以揭示那些逃避傳統沙箱技術檢測的攻擊。
- 點擊時 URL 防護：當使用者點擊惡意連結時，連結會被阻止，以保護使用者免受在電子郵件送達後利用連結進行攻擊的威脅。這與 ESS 中的即時連結追蹤相輔相成。
- Office 365 郵件索回 (clawback)：若後續發現已寄達之郵件其包含惡意軟體，將全數移出最終使用者的收件箱。

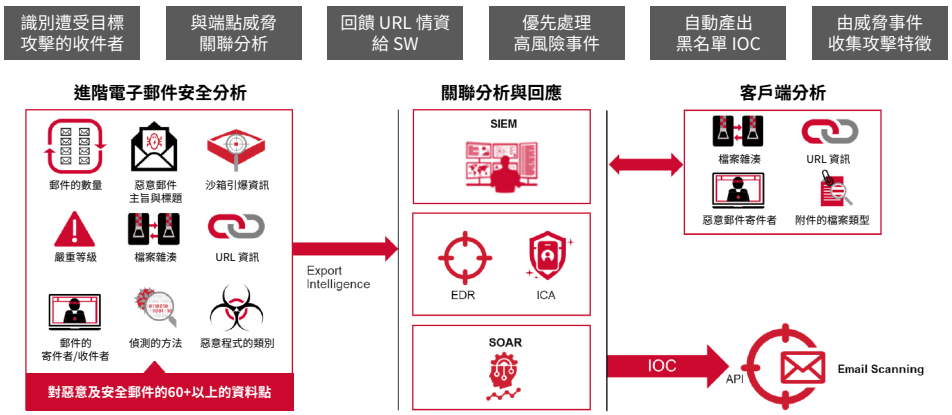
- 網頁瀏覽隔離：透過在使用者與電子郵件連結之間建立一個隔離的執行環境 (類比遠端桌面情境)，保護使用者免受進階電子郵件攻擊 (例如：魚叉式網路釣魚、憑證盜竊和勒索軟體) 的影響，在遠端以唯讀轉譯可疑內容並在交付之前掃描潛在感染的下載。

回應：提供攻擊最深入的能見度，加快對攻擊的應變速度

有效的電子郵件安全不僅僅是預防和隔離，還可以針對目標式攻擊與進階攻擊活動提供更深一層的保護與能見度。Symantec ETDRI 還可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 URL、檔案雜湊和目標式攻擊資訊等資料點獲得比其他廠商更多的入侵跡象 (IOC)。透過提供深度可見性和分析，使得對目標式攻擊和進階威脅的回應更快、更有效。

如圖 2 所示，Symantec ETDRI 透過分析乾淨和惡意電子郵件提供無與倫比的情報，提供超過 60 個入侵指標 (IoCs)，包括 URL、檔案雜湊和目標式攻擊細節。

圖 2：提供進階郵件攻擊最深入的可見性



藉由 API(即應用程式介面)，這些豐富的資料流可以緊密整合到資安營運中心 (SOC) 中，使其與協力廠商的安全資訊與事件管理系統 (SIEM) 以及資安協作自動化應變 (SOAR) 系統相容。

透過這樣的整合，組織可以實現以下目標：

- 搜尋威脅 : 分析您的環境以識別潛在風險，並評估攻擊的嚴重性和範圍。
- 事件關聯 : 使用更多感應器交叉對比各個端點、網路與電子郵件的事件。例如：結合來自 Symantec 端點檢測與回應 (EDR) 和安全網頁閘道 (SWG) 解決方案的洞察，以在多個控制點檢測進階威脅。
- 矯正並協調您的電子郵件威脅防護回應 : 透過將攻擊列入黑名單來遏制威脅，並在您的安全生態系統中自動化回應。

透過將 Symantec 透過將 Symantec ETDRI 與更廣泛的安全框架整合，您可以獲得統一的方法來識別、分析和消除威脅，確保您的組織在面對不斷演變的電子郵件的攻擊時的「資安韌性」。

使用者準備度：強化人性的因素，確實遵守資訊安全措施與相關程序，時時提高警覺

人性的因素是資安防護措施中最薄弱的環節。社交工程即是利用人性容易受騙上當的弱點，破解人性的防火牆，使得使用者在威脅出現時難以識別，直到為時已晚。Symantec ETDRI 提供強大的安全意識和教育能力來應對這一挑戰，大大降低風險並賦予使用戶能夠有效識別和應對電子郵件威脅。

Symantec Symantec ETDRI 讓組織能夠：

- 評估準備狀況：透過可定制的安全評估模擬現實世界的網路釣魚威脅，量身定制以滿足您組織的需求。
- 追蹤和基准進度：詳細的報告和管理儀表板可幫助您對員工準備度的基準作測試，並找出最容易受到攻擊的用戶。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。
- 遵循輕重緩急的郵件安全原則：透過使用 Symantec Information Centric Analytics 獲得深入電子郵件威脅、安全資安事端及使用者行為的廣泛能見度，優先處理對貴公司而言最嚴重的風險。

透過訓練通知提升安全意識，教導使用者應如何識別與回報複雜的電子郵件攻擊。透過為使用者提供檢測網路釣魚嘗試的知識和技能，Symantec ETDRI 建立資安認知文化，降低成功攻擊的可能性，並增強您組織的整體資安韌性。

互通性和相容性：緊密整合以增強安全性

Symantec ESS 與您的整體安全基礎設施 (包括防止資料外洩 (DLP)、加密控制以及端點、網路和雲端安全解決方案) 緊密整合，簡化您的安全性架構並獲得最高投資回報。

Symantec ESS 運用內建的防止資料外洩 (DLP) 和政策式加密控制來攔截、隔離或加密機密的電子郵件，增強合規性和隱私保護工作。

- 防止資料外洩 (DLP)：彈性且內建的 DLP 政策擁有 100 個涵蓋關鍵字字典、一般運算式和 MIME 類型清單的預先定義清單，可識別並控制進出企業的機密電子郵件。
- 政策型加密控制功能：可自動流暢加密特定的離埠電子郵件，確保機密電子郵件的安全和隱私權。這些政策能利用受密碼保護的 PDF 對電子郵件訊息及任何附件進行安全加密， 提供方便行動裝置使用的「推送」加密體驗。

作為賽門鐵克整合式網路防禦平台 (Symantec Integrated Cyber Defense Platform) 的一部分，Symantec ESS 運用內建的防止資料外洩 (DLP) 和政策式加密控制來攔截、隔離或加密機密的電子郵件，進而防止敏感資訊外洩，滿足您在遵循法規及隱私權的需求。這些控制與領先業界的 Symantec DLP 解決方案整合進而強化，能對整個環境內的機密資料 (電子郵件、端點、網路、雲端、行動裝置以及存儲裝置) 進行搜尋、監控與保護。透過此一託管解決方案，組織可以快速部署強大的加密能力，以保護通過電子郵件共用的敏感性資料，而無需管理數位憑證或加密金鑰的複雜性。

該解決方案還與其他 Symantec 產品緊密整合，跨多重渠道進行威脅分析、封鎖、攔截與矯正，進而保護電子郵件、網路以及端點。以增強端點、網路和郵件等多種通訊應用程式的安全性。當與 Symantec 端點安全一起使用時，從新興威脅中收集的電子郵件情報可以作為黑名單分發到端點，防止組織內部的感染。這種相容性將防護功能擴展到現代協作和通訊平臺--包括雲端和本地的 Slack、Salesforce 和 Box，確保安全態勢的統一和強化。

透過將電子郵件安全與您現有的安全生態系統結合起來，Symantec ESS 簡化了管理，增強了威脅回應，並加強了所有數位化接觸點的保護。

摘要

Symantec ESS 能夠整合先進的檢測、隔離、分析和用戶教育，提供對複雜電子郵件威脅的無與倫比的保護。該解決方案使組織能夠在不斷變化的威脅面前保持領先，同時完美整合到您的整體安全生態系統中，以增強合規性、減少操作複雜性並加強整體安全態勢。

賽門鐵克二十幾年來不斷精進，持續推出最準確、有效率且可靠的雲端電子郵件安全服務。Symantec ESS 以領先業界的服務等級協議 (SLA) 為後盾，足見我們對該解決方案的信心，以及提供最可靠的電子郵件安全服務的承諾。Symantec ESS 易於部署、操作和擴展，不管您的企業是處於開始、成長、擴張或是穩定階段，讓你在面對不同階段的挑戰都能提升效率和競爭力！得益於賽門鐵克整合式網路防禦平台 (Symantec Integrated Cyber Defense Platform)，它提供無與倫比的保護、運營效率和較低的總體擁有成本 (TCO)，使其成為保護您的電子郵件基礎設施免受最先進攻擊的理想選擇。

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