Symantec
A Division of Broadcom

解決方案簡介

賽門鐵克電子郵件威脅偵測與回應 (ETDR)

強大的防護功能，能有效遏阻目標式、進階持續性電子郵件攻擊 (APT)，並能全盤掌握您的環境與當前威脅態勢的完整能見度、排定其優先順序並自動化矯正攻擊。

重要功能

- 利用雲端沙箱功能，快速偵測最複雜和隱匿性極高的進階攻擊。
- 透過最強大的惡意 URL 點擊時防護功能 (Click-time URL Protection)，有效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。
- 利用進階電子郵件安全分析，提供郵件攻擊活動最深入的能見度，包括對惡意和乾淨電子郵件超過 60 個資料點的洞察，加快對目標式與進階攻擊的應變速度。
- 藉由整合第三方安全資訊與事件管理系統 (SIEM)，Symantec Information Centric Analytics (ICA) 及 Symantec Integrated Cyber Defense Exchange (ICDx)，快速交叉比對並回應威脅。
- 可以將您在安全環境中搜尋到的威脅，自動將其入侵指標 (IOC) 列入黑名單，此舉能防止新發現的威脅擴散出去，快速矯正電子郵件攻擊。
- 通過內建的安全認知訓練，來減少網路釣魚的風險，該訓練可以讓使用者認識網路釣魚攻擊並做好準備，並幫助組織優先考慮最脆弱的用戶來降低營運風險。
- 交叉比對技術可彙總所有控制點的可疑活動，以識別與排定受到危害且需要立即矯正的系統之優先順序。

有效抵禦最進階的電子郵件攻擊

賽門鐵克電子郵件威脅偵測與回應 (Symantec™ Email Threat Detection and Response：ETDR) 是專為**賽門鐵克郵件安全雲端服務** (Symantec Email Security.cloud) 所提供的**加值進階雲端服務**，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。此服務運用雲端沙箱來對抗最隱匿且進階的電子郵件威脅，利用惡意 URL 點擊時防護功能 (Click-time URL Protection)，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攻擊。此外，ETDR 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)。

透過串流電子郵件安全情報至您的安全營運中心 (SOC)，以快速確定任何針對性或進階攻擊的嚴重性和活動範圍。此外，您可以將搜尋到的威脅，自動將其入侵指標 (IOC) 列入黑名單，此舉能防止威脅擴散出去，快速矯正電子郵件攻擊。而且，ETDR 內建的安全認知訓練，以最新的電子郵件威脅模擬真正的電子郵件攻擊，評估員工是否準備妥當，可以輕鬆地對其進行自定義以滿足組織的需求。最後，與賽門鐵克的端點偵測與回應 (EDR) 和安全網頁閘道 (SWG) 系列一起使用來檢測進階持續性攻擊 (APT) 時，可以自動交叉對比、關聯分析所有控制點 (郵件、端點及網頁) 的事件。然後，可以透過隔離攻擊並將威脅加入黑名單，在整個安全環境中，矯正威脅並讓您做出回應。

由機器學習驅動的雲端沙箱

ETDR 客戶可以利用雲端沙箱，能夠發現並排定現今最複雜的目標式、進階式攻擊優先處理。雲端沙箱運用進階機器學習、網路流量分析、行為分析等先進技術，可以偵測最隱匿的進階持續性威脅。此外，它還融合了世界上最大的民用威脅情報網路 - 賽門鐵克全球智慧型網路的安全監測數據。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 萬個攻擊偵測器的安全監測數據，透過每天分析收集而來的 80 億筆威脅資訊，帶來更優異的安全成效。我們的雲端沙箱還可提供客戶每個檔案的功能和它可執行的動作相關細節，讓所有相關的攻擊元件都能快速獲得調查與矯正。現今有越來越多的進階攻擊「可感知虛擬機器」，也就是說這類攻擊在一般的傳統虛擬機沙箱系統中無法暴露其可疑行為。為了解決這個問題，我們採用了模仿人類行為的技術，也會在實體硬體沙箱執行可疑檔案，以發掘原本可規避傳統沙箱技術偵測的攻擊。

URL 點擊時防護

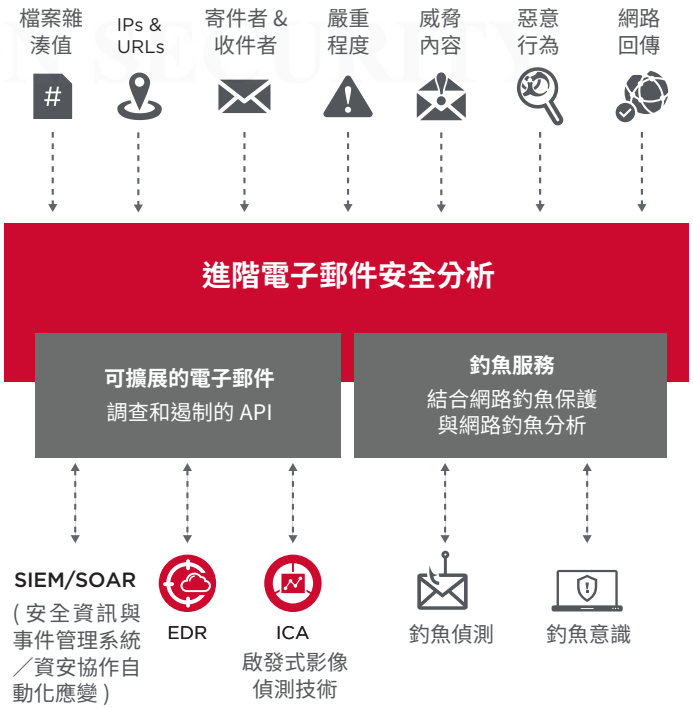
透過 **URL 點擊時防護** (Click-time URL Protection) 分析用戶點擊網頁鏈接，封鎖電子郵件傳送後透過觸發連結發動的魚叉式網路釣魚、目標式與進階攻擊。也是**即時連結追蹤技術**的**配套**方案 (賽門鐵克郵件安全雲端服務的標準防護功能之一)，即時連結追蹤可在傳送電子郵件**前**，封鎖魚叉式網路釣魚攻擊、目標型攻擊和其他進階威脅所使用的惡意連結。與利用特徵檔來封鎖魚叉式網路釣魚攻擊的郵件安全解決方案不同，賽門鐵克搶在使用者點選時即深入評估可疑連結，更可以主動遏止全新及已知的網路釣魚攻擊，深入評估並追蹤至最終目的地，即便攻擊者嘗試使用如多個重新導向、短網址，被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。

進階電子郵件安全分析

ETDR 的進階電子郵件安全分析功能夠更快地回應針對性目標攻擊和進階持續性威脅，從而提供對電子郵件攻擊活動的最深入了解。這種豐富的情報包括對進入組織的每封乾淨和惡意電子郵件的詳細報告。這些報告包括入侵指標 (IOC) 的 60 多個資料點，例如攻擊來源網址，目標攻擊資訊，惡意程式分類，寄件者和收件者資訊，檢測方法，單擊的重寫 URL 以及檔案雜湊的詳細資訊。它可以指出每一次攻擊所屬的威脅類別 (如木馬程式或 Infostealer) 及嚴重性等級 (低、中、高)，以顯示攻擊的複雜等級。Track and Trace 功能可搜尋電子郵件安全雲端服務所攔截惡意網址的進一步詳細資料。其中包括電子郵件中的原始連結，以及透過即時連結追蹤 (Real Time Link Following) 所判斷的含惡意程式之最終目的地連結。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，並且較其他廠商納入更多入侵指標 (IOC)（包括如網址、檔案雜湊、寄件人／收件人資訊、目標式攻擊資訊等資料等超過 60 個資料點）。

圖一：透過 Click-Time URL 防護攔截惡意連結

圖二：透過 Email Threat Detection and Response 深入了解電子郵件攻擊活動



安全營運中心 (SOC) 整合性

ETDR 可以與 Splunk、IBM QRadar、HPE ArcSight 等第三方安全資訊與事件管理系統 (SIEM) 整合，輕鬆地將有關乾淨和惡意電子郵件的進階電子郵件安全分析導出到您的安全監控中心 (SOC)。威脅情報資料通過精細的，由 API 驅動的串流電子郵件安全情報傳輸到 SIEM，從而使您的安全團隊可以快速查看威脅。安全分析師在調查和回應威脅時可以利用這些資料快速關聯和分析威脅。您可以使用免費的 Splunk 或 IBM QRadar 應用程式輕鬆地回應電子郵件威脅，該應用程式允許您將進階電子郵件安全分析直接導出到 Splunk 或 QRadar。這些應用程式通過資料：例如惡意網址、檔案雜湊，例如高風險用戶之類的資訊，傳入攻擊的地理視圖以及電子郵件惡意軟體的時間軸，可以深入了解威脅態勢。

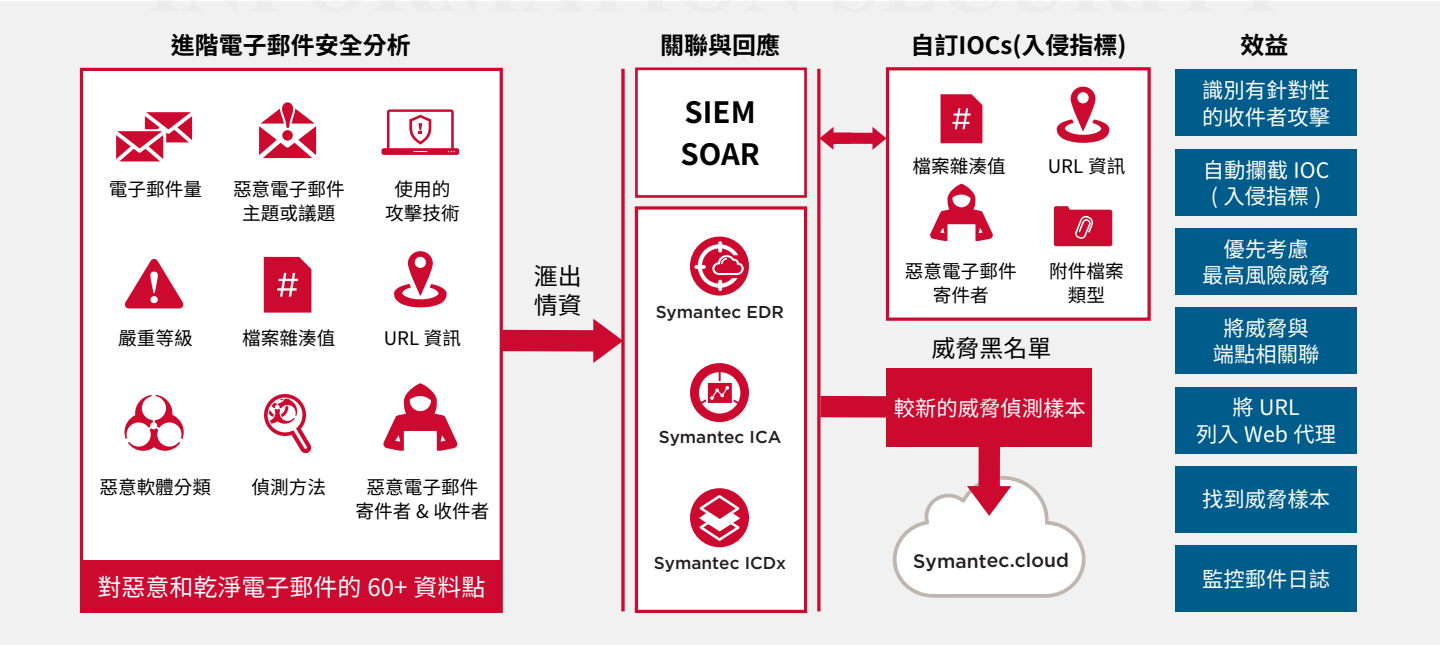
企業可將進階電子郵件安全分析後的數據轉發到 ICA 或 ICDx，可以加快對目標和進階威脅的檢測和回應速度。ICA(Symantec Information Centric Analytics) 獲得深入電子郵件威脅、安全資安事端及使用者行為的廣泛能見度，優先處理對貴公司而言最嚴重的風險。ICDx(Integrated Cyber Defense Exchange) 使企業能夠透過預先建立的元件來簡化資料共享和加速回應操作，以支援多種安全解決方案。

自動化矯正

在回應攻擊或關聯和搜尋環境中的威脅時，安全團隊經常會遇到入侵指標 (IOC)。但是，即使在發現這些威脅之後，矯正措施通常也很緩慢且麻煩，因為入侵指標 (IOC) 通常是手動列入黑名單的。此手動過程會延遲回應時間並增加矯正工作負擔，這對於一次處理數百甚至數千個事件的安全團隊而言至關重要。

ETDR 使您可以通過自動矯正電子郵件威脅來快速回應有針對性的進階攻擊。這些功能通過 API 自動將入侵指標 (IOC)（例如檔案雜湊，IP 地址以及寄件者和收件者資訊）列入黑名單，從而加快了事件回應速度。此外，安全團隊可以通過管理控制台將威脅列入黑名單。將這些入侵指標 (IOC) 列入黑名單可保護您的組織免受新發現的威脅所影響，減少矯正攻擊的時間，並改善整安全狀況，同時提高安全團隊的生產力。如果任何威脅都無法通過我們的防禦，ETDR 會在使用者打開它們之前自動從 Office 365 收件匣中刪除這些電子郵件。

圖三：Symantec 安全運營中心整合



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。

涵蓋所有控制點的整合式檢視畫面

ETDR 可與 EDR(端點偵測與回應) 整合，也能與 SWG(安全網頁閘道) 家族系列搭配使用，以找出可規避個別單一功能產品的威脅。由賽門鐵克龐大的全球情報智慧型網路所提供的情報，ETDR/EDR 可以自動交叉對比、關聯分析所有控制點 (郵件、端點及網頁) 的事件。然後，可以透過隔離攻擊並將威脅加入黑名單，在整個安全環境中，矯正威脅並讓您做出回應。

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政策性整合式解決方案，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