Symantec™ Advanced Threat Protection: Email

產品型錄：**Advanced Threat Protection**

問題

電子郵件一直是進階攻擊進入企業內部一種常見又有效的機制。攻擊者會鎖定選定的受害者，透過電子郵件附加惡意檔案或內嵌連結，以連線至攻擊者控制的網站。他們會利用精密的社交工程詐騙伎倆，誘導疏於防備的使用者開啟惡意電子郵件，而且還會視需要客製化每個攻擊活動，避免受到偵測，進而達到他們的目標。

而這個問題只會日趨嚴重。在 2014 年，每六家大型企業就有五家成為以電子郵件為主的魚叉式網路釣魚攻擊的目標，較前一年攀升了 40%。小型和中型企業遭受這類攻擊的情形也同樣有上升的情況，各增加了 26% 及 30%。[1] 如今現有的安全解決方案顯然不足，無法安全防護企業免於最新型的電子郵件型威脅。

解決方案

由於 Symantec™ Advanced Threat Protection: Email 新增了獨家的目標式攻擊識別及 Symantec Cynic™ 沙箱偵測等功能至現已安裝的 Symantec™ 電子郵件安全雲端服務當中，因此能夠發現透過電子郵件入侵貴公司的進階攻擊。此外，您會收到來自賽門鐵克分析師有關新型或未知惡意程式透過電子郵件入侵貴公司的詳細資訊，以便您判斷任何目標式攻擊活動的嚴重程度和攻擊範圍。同時，當您新增我們的端點或網路模組時，Symantec Synapse™ 交叉比對技術將會自動彙總所有已安裝控制點的事件，為貴公司的重大威脅排定優先順序。

發現並排定進階攻擊的優先順序

Symantec Advanced Threat Protection: Email 能夠發現嘗試透過電子郵件滲透至企業中的進階威脅，並排定其優先順序。此產品可運用並強化現已安裝的賽門鐵克電子郵件安全雲端服務，新增多項重要的新功能找出以電子郵件為主的目標式威脅。

Symantec Cynic™ 雲端沙箱與 Payload Detonation 服務

Symantec Advanced Protection: Email 客戶收到的 Symantec Cynic，是全新打造的雲端沙箱功能與 Payload Detonation 服務，能探索當前極為複雜的目標式攻擊，並排定優先順序。Cynic 運用進階機器學習分析並結合賽門鐵克的全球情報，用以偵測極為隱匿的持續性威脅。Cynic 也提供客戶檔案功能及其執行動作的詳細資料，以便迅速矯正所有相關的攻擊元件。現今有 28% 的進階攻擊「可感知虛擬機器」，也就是說這類攻擊在一般的沙箱系統中不會暴露其可疑行為。[2] 為了與之對抗，Cynic 也會在實體硬體執行可疑檔案，藉此發現原本可規避傳統沙箱技術偵測的攻擊。

1. 2015 年 4 月出版之第 20 期賽門鐵克網路安全威脅研究報告
2. 2015 年 4 月出版之第 20 期賽門鐵克網路安全威脅研究報告

Symantec

Symantec Synapse™ 交叉比對

Symantec Advanced Protection: Email 為完整進階防護產品的一部分，其中也包含了網路及電子郵件控制點的模組。賽門鐵克新的 Synapse 交叉比對技術可彙總所有已安裝控制點的可疑活動，能夠快速辨識遭入侵且需立即矯正的系統，並排定其優先順序。

目標式攻擊識別及詳細的惡意程式報告功能

Symantec Advanced Threat Protection: Email 也能直接運用賽門鐵克研究分析師針對新的目標式攻擊所持續進行的調查結果。此產品將提供嘗試透過電子郵件入侵企業之目標式攻擊的詳細報告，內容包含攻擊技術相關資訊、內含攻擊的電子郵件數量以及電子郵件寄件者與收件者的相關資訊。這項新功能可以協助客戶深入瞭解自身環境中所有目標式攻擊的完整情況。

Advanced Threat Protection: Email 也提供所有內送惡意電子郵件的詳細報告，內容包含 25 個以上的資料點之攻擊活動的深入剖析。這些資料點包含有關攻擊來源網址、惡意程式分類、偵測方法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。

整體來說，這些功能可讓安全分析師將精力和資源投入在對企業而言危險性最高的攻擊上。

透過 SIEM 交叉比對其他資料

Symantec Advanced Threat Protection: Email 可視需求將惡意程式報告資料匯出至第三方的「安全資安事端與事件管理系統 (Security Incident and Event Manager system，簡稱 SIEM)」。藉由經過驗證的網址，幾乎可即時安全地提取最新的 CSV 原始資料。擷取的資訊均包含之前及目前資料請求時間之間所收到的所有資料，以便輕鬆進行差異化資料分析。

針對所有端點、網路及電子郵件遭受攻擊的整合式檢視畫面

Advanced Threat Protection: Email 屬於 Symantec™ Advanced Threat Protection 的一部分，是一套整合式解決方案，可協助客戶發現、排定優先順序並迅速矯正現今最複雜的攻擊。它結合了來自端點、網路、電子郵件以及賽門鐵克龐大的全球偵測器網路所提供的情報，以找出可規避個別單一功能產品的威脅，而這所有的功能都可透過單一管理主控台完成。只要按一下按鈕，Symantec Advanced Threat Protection 就會在整個企業中搜尋、探索並矯正攻擊元件。無需新的端點代理程式。

功能與效益

- 使用 Symantec Cynic 雲端沙箱功能與 payload detonation 服務來偵測複雜又隱密的進階攻擊
- 可接收高度鎖定企業之目標式電子郵件攻擊的詳細報告
- 取得各種惡意電子郵件進入企業的完整報告，包括每次攻擊 25 個以上的特定資料點
- 提供每次攻擊的嚴重性等級，以便對重要性最高的威脅做出更準確的回應。

更多資訊

請造訪我們的網站

http://www.symantec.com/advanced-threat-protection

關於賽門鐵克

賽門鐵克保護全世界的資訊，也是安全、備份與可用性解決方案的全球領導廠商。我們創新的產品與服務能保護任何環境的人員與資訊，從最小的行動裝置到企業資料中心，乃至於雲端系統。我們在保護資料、身分與互動方面領先產業的專業能力，讓我們的客戶在連線世界中充滿信心。如需更多資訊，請造訪 www.symantec.com/zh/tw。

台灣賽門鐵克股份有限公司

地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室
電話：(02) 8726-2000
傳真：(02) 8726-2199
www.symantec.com/zh/tw

21349610-2 11/15