Symantec™ Advanced Threat Protection: Network

產品型錄：**Advanced Threat Protection**

問題

現今的進階攻擊會藏匿於合法網站、運用全新且未知的漏洞、並且透過多種網路通訊協定進入鎖定的企業之中。這些攻擊的設計可避開一般以網路為主的安全偵測方式，因此得以在滲透受害者的基礎架構後危害重要的系統和資料。就算是網路安全產品察覺了這樣的攻擊，詳細的攻擊細節經常會掩蓋在一長串該產品所引發的低優先順序警示之下，使得分析師難以偵測真正的問題所在。

而且這個問題只會日趨嚴重。無論規模大小，幾乎所有的企業都暴露在目標式攻擊的風險之中。在 2014 年，每六家大型企業 (員工人數超過 2,500 名) 就有五家成為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]

解決方案

Symantec™ Advanced Threat Protection: Network 是一套全新的解決方案，客戶可選擇硬體裝置或虛擬機器 (VM) 的形式發現透過網路入侵企業的進階攻擊，並排定處理的優先順序。此產品會自動將所有可疑的檔案傳送至全新的 Symantec Cynic™ 沙箱系統，並可快速偵測最複雜和隱匿性極高的進階攻擊。同時，如果您有 Symantec™ Endpoint Protection 或賽門鐵克電子郵件安全雲端服務，Symantec Synapse™ 交叉比對技術還會自動彙總所有賽門鐵克保護的控制點事件。Symantec Advanced Threat Protection: Network 同時整合了 Symantec™ Advanced Threat Protection: Endpoint 和 Symantec™ Advanced Threat Protection: Email 產品，可提供整個企業的進階攻擊活動整合式檢視畫面。

發現並排定進階攻擊的優先順序

Symantec Advanced Threat Protection: Network 能發現試圖透過常用網路通訊協定滲透企業的進階威脅。現今的網路防護解決方案通常幾乎是完全依賴沙箱功能來找尋攻擊。相較之下，Symantec Advanced Threat Protection: Network 除了創新的 Cynic 沙箱服務之外，還包含了一整套完整的防護功能。此產品包含了 Symantec™ Insight 信譽型技術，可依據檔案首次出現的時間、檔案在網際網路上的普遍性，以及採用數種其他精密技術來辨識可疑檔案。Symantec™ Vantage 可辨識可疑的內送網路流量，並協助尋找網路內與惡意指令與控制 (command-and-control) 伺服器通訊的電腦。此產品會運用賽門鐵克龐大的偵測器網路 (全球規模最大的網路情報網之一) 所提供的情報，以及運用 Symantec DeepSight™ 提供的資料摘要，以確保自身始終能掌握網路上全新攻擊的最新動態。

Symantec Advanced Protection: Network 也包含了賽門鐵克全新的 Synapse 跨控制點交叉比對功能，讓安全分析師得以密切注意最重要的資安事端。

1. 2015 年 4 月出版之第 20 期賽門鐵克網路威脅研究報告

Symantec Cynic™ 雲端沙箱與 Payload Detonation 服務

Symantec Advanced Protection: Network 會將進入企業的任何可疑檔案自動傳送至 Cynic，這是一項全新打造的雲端沙箱和 Payload Detonation 服務，可探索現今極為複雜的目標式攻擊，並排定處理的優先順序。Cynic 運用進階機器學習分析並結合賽門鐵克全球情報，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」，[2] 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。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。

Symantec Synapse™ 交叉比對

賽門鐵克全新的 Synapse 交叉比對技術可運用現有已安裝的 Symantec Endpoint Protection 和電子郵件安全雲端服務，並可跨控制點排定事件的優先順序。舉例來說，假設客戶的傳統網路安全產品偵測到企業中有可疑檔案傳送至員工的電腦。若是使用現有產品時，安全分析師就必須親自使用收到可疑檔案的端點電腦，以確保該檔案在電腦上已經妥善地加以攔截或移除。相形之下，如果 Symantec Advanced Threat Protection: Network 偵測到潛在威脅侵入網路，此產品就會運用 Synapse 交叉比對技術，以自動判定該威脅是否已由 Symantec Endpoint Protection 在端點加以攔截。如果是，該攻擊會在分析師的清單上排定為較低的優先順序。此功能可大幅降低分析師需要檢查的安全事件數量，並讓分析師密切注意可能對企業造成最大風險的可疑活動。Synapse 同時也將彙總並交叉比對所有在賽門鐵克保護的端點、網路和電子郵件的可疑活動，並將此資料融入賽門鐵克龐大的全球偵測器網路，以辨識對企業具有最大潛在危險的重大事件，並排定其優先順序。

運用現有的賽門鐵克投資

Symantec Advanced Threat Protection: Network 可運用您在 Symantec Endpoint Protection 和電子郵件安全雲端服務的既有投資。客戶可在一小時之內即完成部署新安裝的 Symantec Advanced Threat Protection: Network 並開始搜尋攻擊。此產品也會將豐富的情報匯出至第三方的「安全資安事端與事件管理系統 (Security Incident and Event Manager system，簡稱 SIEM)」。舉例來說，該產品可以匯出像是「電腦 A 從網站 C.com 下載了檔案 B.EXE」等豐富資料，而不只是如「已偵測到病毒 BAD.EXE」的傳統安全資料。此外，Symantec Advanced Threat Protection: Network 可由 Symantec™ Managed Security Services 進行監控。

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: Network 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。

重要功能與效益

- 在一小時內即可安裝完成 Symantec™ Advanced Threat Protection: Network 並開始找出攻擊
- 可交叉比對來自現有已安裝的 Symantec™ Endpoint Protection 和賽門鐵克電子郵件安全雲端服務的各種事件，大量減少安全分析師需要檢查的資安事端數量
- 將所有可疑檔案傳送至全新的 Cynic 雲端沙箱和 detonation 服務
- 可採用硬體裝置或虛擬機器 (VM) 的形式

利用賽門鐵克服務讓您的資安處於最佳狀態、將風險降至最低並且獲得最高回報

聯繫安全專家，他們能為您提供進階威脅防護訓練、主動規劃和風險管理，以及為您的企業進行部署、組態設定和評估解決方案。如需更多資訊，請造訪 http://go.symantec.com/services。

[2] 2015 年 4 月出版之第 20 期賽門鐵克網路威脅研究報告

系統需求

適用於此使用者介面的瀏覽器用戶端

Microsoft Internet Explorer 11 或更高版本
Mozilla Firefox 26 或更新版本
Google Chrome 32 或更新版本

虛擬硬體裝置部署環境

VMware® ESXi 5.5、6.0
啟用 Intel 虛擬化技術

虛擬機器 (Virtual Machine，簡稱 VM) 需求

- 四核心處理器 (實體或邏輯)
- 至少 32 GB 的記憶體
- 至少 500 GB 的磁碟空間

實體硬體裝置部署環境

	硬體裝置型號 8840	**硬體裝置型號 8880**
外型尺寸	1U 高機架型	2U 高機架型
處理器	單一 Intel Xeon 六核心處理器	2 個 12 核心 Intel Xeon 處理器
記憶體	32 GB	96 GB
硬碟	1 台 1TB 硬碟	4 台 300GB RAID 5 硬碟
電源供應器	非備援式電源供應器 (PSU)	2 台 750W 備援電源供應器
網路介面卡	4 個 Gigabit 乙太網路連接埠：	4 個 10 Gigabit 乙太網路連接埠 2 個 1 Gigabit 乙太網路連接埠
	1 組 WAN / LAN 1 個管理連接埠 1 個監控連接埠	2 組 WAN / LAN (10 Gigabit) 1 個管理連接埠 (1 Gigabit) 1 個監控連接埠 (1 Gigabit)

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

21349720-2 11/15