產品型錄

賽門鐵克端點偵測與回應 ATP: Endpoint

以單一代理程式偵測並解決進階威脅

一覽

偵測與揭露 – 縮短發現洩漏的時間並迅速揭露入侵範圍

- 採用機器學習和行為分析來揭露可疑活動、偵測資安事端並排列優先順序
- 即時查詢會收集組成資料的證據，直接與端點代理程式通訊
- 自動識別並建立惡意程序檔和記憶體刺探利用行為的資安事端

調查與遏止 – 提高資安事端回應者的工作效率，確保威脅抑制

- 透過持續性記錄端點活動來確保完整記錄資安事端，檢視特定端點的流程
- 即時搜尋所有端點的入侵跡象，尋找威脅
- 以端點隔離的方式在調查期間封鎖可能遭到入侵的端點

解決 – 迅速修正端點，確保威脅不會再次入侵

- 刪除受影響端點上的惡意檔案和相關跡象
- 將端點上的檔案加入黑名單和許可清單
- 增強的報告功能可匯出任何表格作為資安事端解決報告

強化安全性投資 – 預先建立的整合功能及公用 API

- 透過 ServiceNow 應用程式，輕鬆將票證及服務的自動化工作流程延伸至既有的流程中
- 使用針對 Splunk 及 QRadar 預先建立的應用程式，將 EDR 資料和其他安全資訊可視化
- 以 Open API 流暢整合其他安全性產品

簡介

企業正逐漸處於複雜攻擊的威脅陰影之下。事實上，研究已發現威脅潛藏在客戶環境中的平均天數為 190 天[1]。這類進階持續性威脅會利用各種隱藏技術來閃避偵測，繞過傳統安全防線。一旦進階攻擊取得進入客戶環境的管道，攻擊者便能使用許多工具來閃避偵測，並開始刺探利用珍貴的資源和資料。資安團隊在試圖偵測和完整揭露進階攻擊的影響範圍時，會遭遇到許多難題，例如需要人工搜尋分散孤立的大型資料來源、缺乏對於重要控制點的能見度、誤報導致警示疲乏、難以辨識和修復受影響端點。

Advanced Threat Protection (ATP): Endpoint 概觀

Symantec ATP: Endpoint 運用的是 Symantec Endpoint Protection (SEP) 內的整合式端點偵測與回應 (EDR) 功能，可在一小時內部署完成，不需要其他代理程式。調查人員會獲得各種工具，可用於揭露、遏止、解決進階攻擊導致的漏洞 ATP: Endpoint 能夠以精準的機器學習和行為分析技術來揭露進階攻擊。其可將誤報的情況降至最低，讓資安團隊以全球規模最大的民間威脅情報網路 (GIN) 作為後盾，發揮最高的工作效率。ATP: Endpoint 功能可讓資安事端回應者在使用內

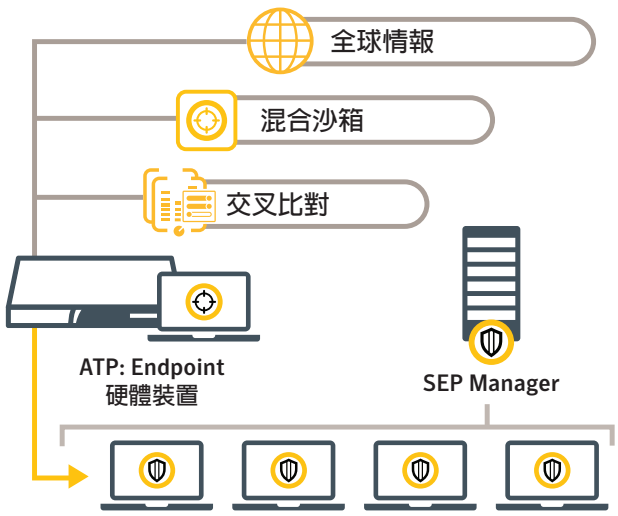
[1] Ponemon 的 2017 年資料漏洞的成本研究報告：美國

部部署或是雲端沙箱調查威脅時，也迅速地搜尋、識別並遏止受影響的端點。此外，系統活動的持續性記錄功能足以支援完整的端點能見度和即時查詢需求。且 ATP: Endpoint 可在單一主控台上一按便從受影響的端點刪除惡意軟體和相關跡象，確保解決漏洞威脅。

偵測威脅 – 故意躲得「顯而易見」的威脅也逃不掉

ATP: Endpoint 使用多種方式來偵測進階威脅。先進的機器學習和行為分析技術可辨識惡意和可疑的檔案。且 ATP: Endpoint 會偵測透過記憶體的刺探利用和 PowerShell 程式檔來入侵的無檔案攻擊。

ATP: Endpoint 以 SEP 代理程式提供偵測與回應功能



提高調查人員工作效率

ATP: Endpoint 可根據風險等級來排定資安事端的優先順序，藉以提高調查人員的工作效率。ATP: Endpoint 還會自動針對賽門鐵克的動態攻擊者情報辨識出的目標式攻擊來產生資安事端。

此外，調查人員也可以利用端點活動記錄功能來追蹤攻擊跡象並執行端點分析。ATP: Endpoint 所支援的事件隨選擷取的範圍相當大，包括階段作業、流程、模組載入點修改、檔案與資料夾操作、登錄變更、網路連線活動等。

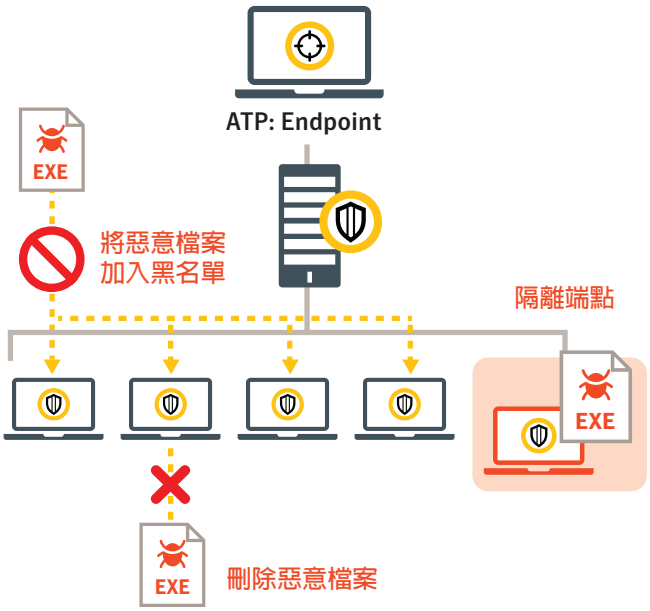
根據 Symantec Internet Safety and Threat Report (ISTR) 所述，超過 20% 的惡意軟體具有虛擬機器感知能力，也就是可躲開傳統沙箱的偵測功能。ATP: Endpoint 採用多種進階技術 (包括模仿人類行為)，可偵測出此種能夠感知虛擬機器的威脅，如有必要可使用實體伺服器加以觸發。

ATP: Endpoint 提供智慧型資安事端警示，可提高調查人員的工作效率

快速修正端點

ATP: Endpoint 可迅速修復受影響的端點，包括檔案刪除、加入黑名單、端點隔離。若使用 ATP: Endpoint，應變人員要採取行動時只需在單一主控台上一按，便能在多個端點上套用修正方法。

ATP: Endpoint 讓資安團隊可在幾分鐘內對進階攻擊作出回應



涵蓋多個重要控制點進行交叉比對

ATP: Endpoint 屬於規模更大的 Advanced Threat Protection (ATP) 平台的一部分，可提供能見度並交叉比對來自網路和電子郵件模組的事件。ATP: Endpoint 硬體裝置自動將來自 SEP、電子郵件、網路活動的事件進行交叉比對。賽門鐵克的 ATP 模組 (ATP: Endpoint、ATP: Network、ATP: Email) 可使用單一代理程式在一個主控台上進行威脅的偵測和排定優先順序。

Symantec Advanced Threat Protection	**ENDPOINT**	揭露、調查、解決涵蓋所有端點的攻擊危害	運用 Symantec Endpoint Protection
	NETWORK	使用多層式技術防止並偵測入侵網路的進階威脅	虛擬或實體裝置
	EMAIL	保護並偵測透過電子郵件入侵網路的進階威脅、找出目標式攻擊。	運用沙箱與電子郵件安全性雲端

重要的 3.0 功能

端點活動記錄器

涵蓋 SEP 端點的持續性能見度

- 記錄重大系統活動，包括檔案作業、登錄金鑰變更、流程活動、載入點變更、使用者登入及登出
- 選出重點事件，以啟發式技術和專家規則進行進一步的分析和資安事端生成

端點分析

搜尋、篩選、擷取特定端點的事件

- 直接搜尋 EDR 資料庫和端點
- 資安事端調查人員可迅速篩選特定屬性、辨識不尋常的數值並轉向相關的實體頁面
- 擷取特定端點的流程事件以供分析

無檔案的威脅偵測

偵測並檢視可疑的程序檔以及對記憶體的刺探利用

- 檢視 PowerShell 流程、規則型偵測識別作業、建立針對惡意程序檔的資安事端
- 自動為 Symantec Endpoint Protection 封鎖的記憶體刺探利用行為產生資安事端，以供調查人員分析相關跡象

混合沙箱

於內部部署或雲端上觸發檔案

- 使用雲端型或內部部署的沙箱觸發可疑檔案
- 支援實體和虛擬的可疑檔案感知功能
- 運用檔案信譽、網路流量分析和全球遙測技術

增強的公用 API 和全新的整合功能

減輕自訂整合的難度並運用預先建立的元件

- 全新的公用 API 支援多種新功能，包括端點活動記錄器功能
- 為熱門的 SIEM 及 ITSM 解決方案 (Splunk、QRadar、ServiceNow) 提供預先建立的元件
- 以 Active Directory 使用者和群組來存取主控台

系統需求

Symantec Endpoint Protection 14.X、Symantec Endpoint Protection 12.1 RU6 MP7 (僅 SEP 14 及更高版本的 ATP: Endpoint 支援記錄器)

伺服器規格			
外型尺寸	**8880**	**8840***	**VMware ESXi**
	2U 高機架型	1U 高機架型	虛擬機器
處理器	2 x Intel Xeon E5-2697 v4	E3-1270 V5 、3.6GHZ、4C/8T、80W	12 個 CPU
記憶體	192 GB	32 GB	48 GB
硬碟	RAID 10、4 台 300GB 15K SAS 硬碟 RAID 10、4 台 1.8TB 10K SAS 硬碟	RAID 1、2 台1 TB 7.2RPM NLSAS 12GBPS 2.5” 吋硬碟	500 GB (應額外再擴充 1 TB 以支援端點活動記錄)
網路介面卡	4 個 1GbE 乙太網路連接埠 4 個 10 Gigabit 乙太網路連接埠	2 個 1GbE 乙太網路連接埠	2 個 1GbE 乙太網路連接埠
DVD-ROM	DVD ROM、SATA	DVD ROM、SATA	無
電源供應器	2 個 750 W 備援電源供應器	2 個 750 W 備援電源供應器	無

*8840 硬體裝置不支援端點活動記錄

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 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策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。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 www.symantec.com.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.tw