Symantec Endpoint Protection 被譽為評估端點防護的標竿

前言

賽門鐵克是資安業的長青樹，品牌享譽至今近四十年。自 2019 年被全球網通晶片巨擘--博通 (Broadcom) 合併後，特別是以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。保安資訊長期專注在 Symantec 解決方案的專業與經驗，在業界備受推崇，我們一貫的信任、尊重、誠實、尊嚴、禮貌、舒適的對待顧客準則，是 貴司值得長期信賴的資安夥伴！

1. **惡意程式防護技術**：具備檔案型特徵檔比對技術、檔案及網頁信譽、進階機器學習、啟發式、入侵預防、主機型防火牆、行為偵測、網路保護、政策鎖定等兼具可靠、穩定、有效與創新技術，能有效抵禦病毒、蠕蟲、間諜程式、零時差、社交詐騙、勒索軟體、目標式鎖定攻擊、進階持續性威脅、偷渡式下載並大大降低單靠行為或機器學習等標榜創新技術所造成的誤判。有興趣可參考原廠技術白皮書：最新賽門鐵克的 STAR 惡意程式防護技術。
2. **降低受攻擊面政策強制功能**：裝置控管、應用程式控管、主機完整性檢查、系統鎖定、防護軟體自身避免被停用保護功能。就如同有小嬰兒的家庭一樣，會把一些危險的瓶瓶罐罐、剪刀、藥物、熱水瓶、熱湯、設法遠離小嬰兒。而降低受攻擊面政策強制功能，就是讓資安認知較薄弱的用戶，遠離威脅或感染媒介。
3. **全世界最大的民間資安情報庫**：賽門鐵克全球情資網路(Symantec Global Intelligence Network：GIN)分析超過9PB(PB=2的50次方)的海量安全威脅資料，讓我們的系統和專家能夠快速精準地識別和檢測威脅，確保我們的客戶免受任何攻擊。它推動我們的行業領先的技術，為您的業務提供更全面的保護。有興趣可參考相關資訊圖表及線上研討會簡報檔：賽門鐵克全球情資網路(GIN)--資訊圖表／賽門鐵克全球情資網路(GIN)--隱身在賽門鐵克資安解決方案背後的強大力。
4. **主機完整性檢查**：可設定病毒定義檔不符合、系統修補版次不符合、登錄檔機碼不符合、是否登入 AD…等眾多環境或安全因子，則依設定自動套用攔截、隔離及矯正的處置政策。主機完整性賦予資安人員、技術顧問更多力量與資源，更能自主掌控與強化企業內部的端點安全等級。
5. **入侵防護(IPS)**：支援已公開之漏洞型攻擊，類似行為之零時差攻擊亦能防護，並支援無檔案型態 (Fileless) 及 URL 信譽識別，可辨識網域和 URL 的威脅，於受支援的瀏

覽器上可阻擋惡意網頁。有興趣可參考原廠的線上研討會簡報檔：讓網路威脅未攻先破--賽門鐵克的 IPS 入侵預防技術。

6. **記憶體攻擊緩和**：可阻止對廠商尚未在 Windows 電腦上進行修補的常用軟體應用程式的攻擊。記憶體攻擊緩和使用各種緩和技術來偵測侵入嘗試。為了阻止侵入，記憶體攻擊緩和會將 DLL 插入至受保護的應用程式。在記憶體攻擊緩和偵測到侵入嘗試之後，它會攔截刺探利用或終止刺探利用所威脅的應用程式。

7. **主機型防火牆**：具備網路層 (IP) 及應用層 (Application) 防禦及管理功能，防止任何未獲授權的使用者存取組織中連線到 Internet、監控您的電腦與 Internet 的通訊、建立防護措施，允許或攔截他人企圖存取您電腦上的資訊、警告您來自其他電腦的連線嘗試警告您電腦上的應用程式嘗試連線到其他電腦。

8. **竄改防護功能**：能保護 SEP 代理程式不被停用並告警遭停用的嘗試，許多短時間大規模的致命性攻擊，第一個動作就是關閉端點防護 (或防毒軟體)，讓後續的攻擊鏈可以神不知鬼不覺地被完成。SEP 的竄改防護功能，能有效避免這種大災難。

9. **用戶端平台相容性**：現有支援／最新版本可安裝並正常運作於 Windows 7~Windows 11、Windows Server 2008~Windows 2022、Linux 以及 Macintosh。用戶端無須重新開機即有最新防護完整功能。如果採購 SESE 或 SESC 版本，則可新增 IOS／Android 的防護功能。

10. **管理主控台平台相容性**：最新版本可安裝並正常運作於 Windows Server 2012-Windows Server 2022 並支援HA架構。資料庫支援 MS-SQL 或 MS-SQL Express。如果採購 SESE 或 SESC 版本，則可免費使用原廠雲端主控台而無須自建。

11. **管理主控台功能**：能依不同群組，套用第 1 及第 2 項等相關防護技術及遵循管理、安全防護、通報示警…等最佳政策，亦能鎖定用戶端的互動（自行操作）功能，避免用戶端自行移除或停用相關功能。

12. **病毒定義檔更新機制**：支援管理主控台自動派送、連線至原廠全球更新主機自動下載更新、SEP 用戶端電腦也能設定為內容更新主機讓網內電腦更新、無法上網或無法與內網連線之隔離電腦亦可下載自動更新程式點擊後自動更新、不接受控管之電腦亦可連線至內部自建內容更新主機，避免對外連線網路頻寬消耗。

13. **完整的後送機制及應變措施可避免自行開發或罕見的乾淨軟體誤攔**。有興趣可參考說明文件：Symantec Endpoint Protection 的誤判預防與修正。

14. **原廠提供病毒樣本後送分析之機制**。

15. **原廠提供系統診斷工具**收集防護軟體相關日誌，以利除錯和疑難排解資訊。

16. **防護擴充延伸功能**：舉凡提升具備端點偵測與回應 (EDR) & 專業沙箱檢測功能、AD 防護、具備隨機應變的自適應防護Adaptive Protection、Web 和雲端存取防護可讓您將流量從 Symante Agent 重新導向到 Web Security Service，從本機延伸到網路級防護等創新防護技術，都不需再重新安裝任何用戶端代理程式，讓企業可以無縫接軌，快速順暢提升最高等級的端點安全。

17. **第三方安全管理協作擴充功能**：開放的 API 支援主流 SIEM 及 SOC 分析平台，非常適合大型企業或委外資安服務業者。

18.**美國全國性聯合防禦計畫 JCDC (Joint Cyber Defense Collaborative)成員**：2021年8月，因應國外發動的針對性攻擊日益嚴重，美國拜登政府網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫JCDC (Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。

19.**最新兩個版次的新增或強化功能說明**：SEP 14.3RU7／SEP 14.3RU8 (最新)。除非現有使用中版本有安全瑕疵，否則安裝最新版次未必是最適合特定情境的版次，企業環境有許多考量面向，建議先與保安資訊聯繫可獲得面面俱到的周延建議。

20.**SEP14.3RU3之後，特別針對最新加密勒索軟體防護技術的強化**：

- 針對 Conti、Avoslocker 和 Hive 等常見勒索軟體家族，能提供特別防護的能力。
- 具備就地取材攻擊 (LOTL) 常被濫用的系統管理工具、第三方管理工具以及安全評估與監測軟體或紅隊工具提供預防保護。
- 具備偵測勒索軟體攻擊中所使用之初始存取和水平擴散技術。
- 可防護 Cobalt Strike 所使用的程序插入技術。
- 具備偵測 Emotet 垃圾郵件活動能力。
- 防禦 IcedID 這類高感染狀況惡意程式。
- 偵測目標勒索軟體攻擊中使用的可疑程序鏈。

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588