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！

☑**涵蓋攻擊前的降低攻擊面、事前預防、事中處置與事後檢討改善的業界最完整端點安全解決方案**：賽門鐵克端點安全解決方案共有三個料號 (SEP／SESE／SESC) 可以完全涵蓋事前預防、事中處置與事後檢討改善的所有端點安全的環節。過往大家認知的防毒軟體，其實只著重在「事中處置」，也就是數以千萬計的電腦病毒、惡意程式已經兵臨城下了，才來查找並刪除，一定會有漏網之魚而釀成災害。本文所介紹的多種防禦技術，應該只有「惡意程式防護技術」這一項是屬於防毒軟體的範疇，其他的防禦技術與安全管理機制多側重在降低攻擊面、防患未然，以及強化或延伸惡意程式防護技術的質量與綜效。而 EDR 對於事後檢討改善非常有幫助，同時對所有端點的即時安全可視性(安全監視)，也是受到高度監管的行業以及法規遵循要求嚴謹的產業必要的資安防禦與安全管理架構。而 Symantec 的 AD 防護的底層邏輯則是利用欺敵技術、聯合所有的端點來保護 AD 的聯防策略， 優勢則是可避免傳統在 AD 主機直接安裝AD 防護軟體的一夫當關，萬夫莫敵的單項弱點風險 (Single point Vulnerability)。整體而言，賽門鐵克的端點安全解決方案具備能應對各種複雜問題的靈活度，以及容易運用的特性。

☑**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 (身家調查)、進階機器學習 (AML)、人工智慧 (AI)、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分析、機器學習 (ML) 或人工智慧 (AI) 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。

☑信譽分析 (Reputation)：Symantec Insight 是一種安全技術，能夠調查檔案相關資訊，使用檔案老舊程度、頻率、位置和其他資訊，以找出其他方式無法找出的威脅。Symantec Insight 根據 200 個以上國家／地區超過 1.75 億個系統所建置而成，能夠檢查並追蹤檔案的相關資訊。賽門鐵克獨特的信譽分析會使用情報網路交叉比對上百億的使用者、檔案與網站間的數百億個關聯，可主動攔截更多威脅，抵禦快速變種的惡意程式。透過分析幾項關鍵檔案屬性，例如：檔案的下載次數、存在時間及下載來源，我們就能準確地偵測檔案的好壞，並在檔案到達端點前為每個檔案指定信譽評等。還可根據檔案信譽僅掃描有風險的檔案，有效地大幅減輕高達 70% 掃描負荷。自行變形和加密的惡意程式也無法躲避偵測。

☑進階機器學習(Advanced Machine Learning)：端點上的多面向機器學習可防止新型和未知的威脅，減少對病毒特徵的依賴。使用全球情報網上數以兆計的好壞檔案樣本來訓練機器學習，以大幅降低誤報率。這種進階機器學習技術會由我們的威脅專家持續訓練和微調。賽門鐵克將此技術與多層式防護結合，加上全球威脅情報，可以有效杜絕未知惡意程式和零時差威脅。機器學習是目前被公認為最高偵測率的防毒技術，副作用是有較高的誤判率，目前標榜機器學習技術的新創公司，誤判率的平均水準約在 10% 左右，而賽門鐵克的機器學習是同時與後端的全球最大智慧型威脅資料庫查詢 (Symantec Global Intelligent Network)，所以準確度高達 99.9%，為業界最低的誤判率。也就是說 SEP 14 用機器學習技術來提升高偵測率，由多種定義檔來確保最低的誤判率並維持最高的效能。

☑行為監控(Behavior)--SONAR主動式行為防禦技術：雖然有極少數威脅在現階段仍無法偵測，Symantec Endpoint Protection 的行為監控還是非常有效。此技術運用機器學習來提供零時差的防護，可在程式執行時，即時監控將近 1,400 種檔案行為並判斷檔案風險，有效地防止新型和未知的威脅。

☑強而有力的反藏匿技術--模擬(Emulator)：許多惡意程式會採用包裝 (Pack) 的藏匿技術，將自己隱藏起來。SEP 14 新增的高速模擬 (Emulator) 技術，算是新型的沙箱技術，能透過變種的自訂套件，偵測隱藏的惡意程式。靜態資料掃描程式會在輕量型虛擬機器上，以毫秒的速度掃描每個檔案，使威脅無所遁形，同時協助改善偵測率和效能。

☑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。

☑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^{50}) 的海量安全威脅資料，並且隨時更新，擁有數量、速度以及多樣性的優勢。也讓需要大型資料集才能進行訓練的 AI 防護機制，能如虎添翼。GIN 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。它推動了我們的行業領先的技術洞見，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。

☑**主機完整性檢查**：任何事故的根本原因不外乎為該作的沒作 (例如：變換車道不打方向燈) 或有作卻作錯 (例如：錯把油門當成剎車)。主機完整性檢查就是在檢查：該作的事有沒有作？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……等眾多必要的環境或安全因子進行檢查，如果不符合，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。對系統熟捻的 IT 專家，特別喜歡利用它來查找異常的機碼或檔案，對分析全局的異常，非常快速。

☑**入侵防護(IPS)**：IPS 攔截的威脅數量，約佔所有防護技術的 70%，是比惡意程式防護技術更重要元件。它是基於網路封包拆解／分析／過濾的防護技術，早在 2003 年就是賽門鐵克領先業界突破性技術。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，可阻擋惡意網頁、惡意表單詐騙、惡意網址重導向、惡意 C&C 連結、技術支援詐騙嘗試……。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 入侵預防技術或部落格文章：賽門鐵克端點上的網路保護技術有何過人之處？

☑**記憶體攻擊緩和**：這項防護技術的底層邏輯就是--只有特定的鎖匙 (漏洞利用工具) 才能開啟特定的鎖頭 (漏洞)。所以針對已揭露的漏洞，我們就會在第一時間拆解並分析所有可能的攻擊模式，而不是等相同漏洞有新的攻擊模式出來，才來事後提供特徵檔。只要是已經揭露的漏洞就有相對應特定的漏洞利用工具的特徵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。記憶體攻擊緩和能使 Heap Spray、SEHOP 覆寫和 Java 攻擊等零時差攻擊失去效力，以保護廠商尚未發佈修補程式的常用軟體，避免威脅。無論任何瑕疵、程式錯誤或漏洞，這項非病毒特徵型技術都能發揮效用。

☑**主機型防火牆**：具備網路層 (IP) 及應用層 (Application) 防禦及管理功能的主機型防火牆 (Host-Based FireWall)，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。主機防火牆的另一項功能，類似大樓的防火門 ，可稱是安全門，其具有一定的防火時效，所以可以暫時將火災產生的煙和熱阻隔在防火門外，以確保安全梯內成為無火、無熱、無煙危害的安全空間。

萬一在企業內部發生疑似內部攻擊時，用戶端防火牆是一個非常好用的自我保護與自我隔離機制，可以馬上停止所有的網路服務，讓內部攻擊無法再亂竄。

☑**竄改防護功能**：能自我保護 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。

☑**裝置控管(Device control)**：限制特定硬體的存取權限，並控制哪些類型的裝置可上傳或下載資訊。亦可將外部媒體控管與應用程式控管結合，以提供更具彈性的控管政策。妥善使用應用程式與裝置控管，就能藉由監控應用程式行為，以及對檔案存取、系統登錄檔存取、允許執行的程序以及可寫入的裝置資訊進行控制，協助防止內部與外部的安全漏洞。最簡單的應用就是只接受 USB 的鍵盤／滑鼠，其他隨身碟或手機都無法連接接到電腦上。

☑**應用程式行為控管(Application control)**：控管檔案、系統登錄的存取以及處理程序可執行的方式。妥善使用應用程式與裝置控管，就能藉由監控應用程式行為，以及對檔案存取、系統登錄檔存取、允許執行的程序以及可寫入的裝置資訊進行控制，協助防止內部與外部的安全漏洞。

☑**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 2025、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。賽門鐵克是資安一線廠商，與全球軟體巨擘緊密協作構成的生態系，總能在第一時間推出最穩定相容的版本。近期多家因資安事件而上報的機構組織，多有因還有 Windows 7 應用於產線或醫療儀器設備，不乏採用高價解決方案卻無支援 Windows 7 而成為資安破口的憾事。

☑**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 2025 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。

☑ **簡單易懂且易於管理的中央主控台**：能依不同群組，套用最適化的不同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。管理主控台依購買端點防護產品的不同 (SEP／SESE／SESC)， 可分為地端自建與原廠雲端主控台。企業環境需要有中央主控台的機制來監視整體端點的資安健康度，像是誰把端點安全軟體停用、移除以及異常偵測到特別多的惡意程式或存取惡意網站，這些異常往往是企業資安災難的初期的破口及導火線。

☑**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。

☑**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。

☑**原廠提供病毒樣本後送分析之機制**。
Symantec 疑似誤報檔案遞交網址
https://symsubmit.symantec.com/false_positive
Symantec 可疑檔案(疑似漏攔)遞交網址
https://symsubmit.symantec.com/false_negative

☑**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**。

☑**最方便的防護擴充延伸功能--單一代理程式**：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 等創新防護技術，都不需要再重新安裝任何用戶端代理程式，可以降低評估其他解決方案對現有穩定的生產環境的可能風險以及資安架構的複雜度、讓企業可以無縫接軌，快速順暢提升最高等級的端點安全。EDR 具備化繁為簡，快速幫助資安人員了解問題所在，進而獲得更大的成效。

☑**自適應防護(Adaptive Protection)**：這幾年駭人聽聞的資安事件60%以上都有採用就地取材攻擊 (Living-off-the-Land，LOTL) 手法，而且與日俱增。駭客利用受害電腦裡現成的工具，來執行攻擊行動的有關任務，這種手法被稱作「Living Off-the-Land (LOTL)」，目的是藉由這些合法工具來掩護非法行動。在前十大勒索軟體攻擊者愛用的工具當中，有 6 款是 LOTL 工具，包括 PsExec、Powershell、WMI、VssAdmin、Reg.exe 以及 Net.exe，由於這些是系統管理者每日用來監控及維運系統的工具，因此資安產品不能直接阻擋。自適應防護技術是透過 AI 及機器學習來減少被攻擊管道，它透過不斷分析用戶的操作情境，來辨識哪些是 IT 人員正常使用 LOTL 工具的行為、哪些是由駭客所操作，並且能提出建議關閉未曾使用的工具和應用程式，以限縮可能被用於攻擊的管道。然而由於每家企業 IT 團隊運用 LOTL 工具的方式不盡相同，因此管控方法無法一體適用，賽門鐵克的自適應防護技術提供精細的行為分析及各種行為相對應的控制措施，大幅降低 LOTL 工具成為駭客入侵的可能，同時讓正常的 IT 營運不中斷。

＊**特別註明**：SEP 14.3 RU10 版次，已將這個功能納入，之前只包含於端點安全完整版 SESC。地端自建 (SEP) 與雲端主控台 (SESE／SESC) 所提供的自適應防護功能有些許不同，可參考比較表。

☑**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。

☑**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。

☑**實現端點安全可信度的人員(People)、流程(Process)和技術(Technologies)**：資安防護的工作其實跟減肥計畫很像，再貴

再好的減肥藥還是要搭配規律的運動以及適度的飲食控制。再好再貴的端點防護系統還是需要有專業度強、態度積極的維運人員，才能發揮防護系統的最大效用。同時也要兼顧現有生產力軟體的運作順暢，避免造成干擾。「事前預防」勝於「事後處理」被公認為資訊安全的第一性原理，以艾森豪矩陣 (或稱優先矩陣) 的重要／緊急四象限分類法，平常就應該把預防 (重要但不緊急) 的措施做好，降低救火 (重要但緊急) 的機率，並具備在小問題還沒惡化成大麻煩的黃金時間之警覺、反應、應變的知識與能力。賽門鐵克的端點防護技術，能完全涵蓋攻擊鏈各個階段所需的有效、穩定、可靠以及與時俱進的先進技術、配合資安流程所需的政策強制以及管理功能。保安資訊提供的教育訓練、知識傳授以及經驗分享，多能協助組織培養所需的資安系統維運人才。我們樂於與我們的客戶緊密協作，來優化最適合的安全政策與防護策略。事實證明，一直以來，都沒有不需要人員投入就能提供最佳防護的系統，否則資安事件上新聞的主角，不會三不五時是肯花大錢又使用廣告做很大之資安品牌的客戶。

☑最新兩個版次的新增或強化功能說明：SEP 14.3RU9／SEP 14.3RU10 (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～找專家、省時間、保成功。

☑SEP14.3RU3之後，特別針對最新加密勒索軟體防護技術的強化 (歷次與時俱進的進化紀錄)：

- 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。以僅是初版的示例，欲了解歷次與時俱進的進化紀錄，請點擊此處。

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)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合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。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國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。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。