Symantec
A Division of Broadcom
解決方案簡介

SES 賽門鐵克端點安全

實作端點安全策略一致性的重要程度更甚以往

賽門鐵克端點安全完整版 (SESC:Symantec Endpoint Security Complete) 重要功能

- 為所有端點提供保護：筆電、桌機、平板、手機以及伺服主機
- 單一代理程式提供涵蓋攻擊狙擊鏈不同階段的安全：攻擊面降低、攻擊預防、入侵預防以及偵測與回應
- 單一主控台提供即時的威脅可視性／能見度
- 靈活的佈署方式：地端自建、雲端管理以及地端雲端混合模式
- 主動目錄 (AD：Active Directory) 安全
- 基於行為模式的應用程式隔離與應用程式控制功能
- 基於人工智慧 (AI) 指引的安全管理
- 目標攻擊分析與威脅搜尋
- 全球情報網絡 (GIN) 是賽門鐵克所營運的全球最大民營資安威脅資料庫，可提供即時的威脅資訊、威脅分析、內容分類和全面的威脅阻止資料庫
- 開放式的整合框架：經由賽門鐵克整合式網路防禦交換平台 (ICDx)，可與第三方廠商包含 Microsoft Graph、Open C2 以及賽門鐵克自有多元解決方案整合

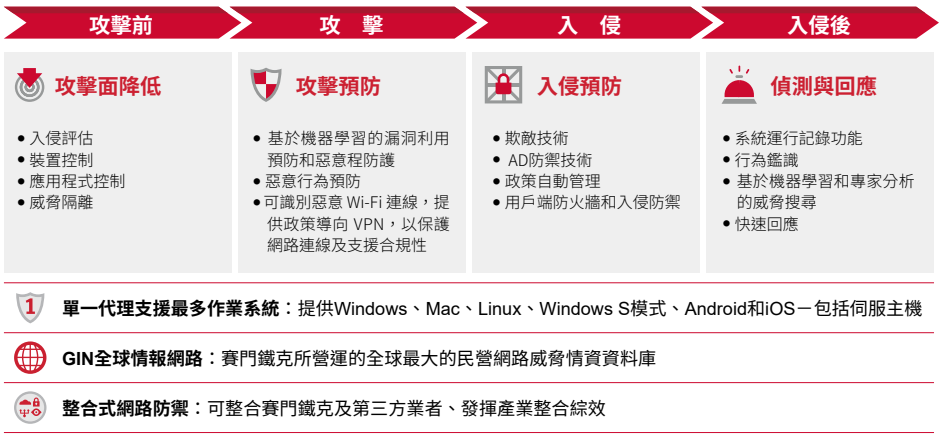
簡介

端點是網路攻擊者的主要目標。隨著攻擊事件的爆發式成長與造成的災損失屢創新高。許多公司為了做出回應，嘗試新增多種端點防護產品，以擴大整體防禦。可惜這種方式實際上會減弱組織的安全態勢。

Ponemon Institute 發現，組織平均安裝七種不同的端點代理程式，以支援 IT 管理及安全[1]。 每種代理程式都在自己的主控台獨立運作，擁有自己的一套規則和政策，全部都需要進行政策及功能設定、安裝佈署、管理及維護。多種產品除了造成更多 IT 負擔及成本，也會產生防禦缺口及錯誤，增加您遺漏威脅的可能性。

預防至關重要，因為全球網路威脅比以往任何時候都更具侵略性，並且可能對企業產生巨大影響。在您花時間閱讀此資料表時，整個企業可能會受到損害。據報導，NotPetya 襲擊僅數 7 分鐘[2] 就使全球最大的航運公司之一與數以千計的其他組織一起癱瘓。儘早防止攻擊至關重要，因為現代化攻擊的偵測和回應的時間非常短。投資事件回應對於建立強化的安全狀態以防止將來的攻擊也至關重要。賽門鐵克可協助您不再妥協。如果能同時享有最佳安全及最簡單的方法，為何要從中做出取捨？

圖一：賽門鐵克端點安全完整版 (SESC)



1: The 2017 State of Endpoint Security Risk, Ponemon Institute LLC, November 2017.
2: *You're Just 7 Minutes Away from an Infinite Toxic Loop in Your Network*, Symantec Blog, April 2019.

賽門鐵克端點安全企業版 (SESE:Symantec Endpoint Security Enterprise) 重要功能

- 為常用的端點提供保護：筆電、桌機、平板、手機以及伺服主機
- 單一代理程式的端點安全
- 單一主控台提供即時的威脅可視性 / 能見度
- 靈活的佈署方式：地端自建、雲端管理以及地端雲端混合模式
- 基於人工智慧 (AI) 指引的安全管理
- 全球情報網絡 (GIN) 是賽門鐵克所營運的全球最大民營資安威脅資料庫，可提供即時的威脅資訊、威脅分析、內容分類和全面的威脅阻止資料庫
- 開放式的整合框架：經由賽門鐵克整合式網路防禦交換平台 (ICDx)，可與第三方廠商包含 Microsoft Graph, Open C2 以及賽門鐵克自有多元解決方案整合

解決方案概述

賽門鐵克端點安全完整版 (SESC) 提供全球最完整的整合式端點安全平台。賽門鐵克平台採用單一代理程式，可作為內部部署、雲端型以及混合型解決方案，協助保護所有傳統及行動端點裝置，在裝置、應用程式及網路層級提供連鎖防禦，並使用人工智慧 (AI) 實現最佳安全決策。統一的雲端型管理系統可簡化防護、偵測及回應所有鎖定端點的進階威脅。

為組織提供無與倫比的端點安全

賽門鐵克在攻擊過程的三個階段（攻擊前的準備階段、攻擊階段和攻擊後續階段) 為傳統和行動裝置提供了最佳的端點安全性，強調是在整個攻擊鏈中進行預防以實現快速遏制。 主動的攻擊面減少和創新的攻擊防禦技術可為最難檢測到的威脅提供最強大的防禦，這些威脅依賴於隱形惡意程式，憑證盜竊，無檔案式的隱匿攻擊，結合「自給自足」戰術 (即利用常見 IT 工具進行攻擊)，賽門鐵克還可以在發生滲透之前防止全面破壞。先進的攻擊分析、行為取證、自動化調查教戰守則和業界第一套保護 AD 遭橫向移動、憑證防盜，提供精確的攻擊檢測和主動的威脅搜尋，以遏制攻擊者並即時解決持續存在的威脅。

攻擊面減少

賽門鐵克提供了基於進階政策控制和先進技術，能大大降低攻擊面的主動式端點防禦機制，可連續掃描應用程序、Active Directory 和裝置之間的漏洞和錯誤配置，讓駭客的戰術和技術無用武之地。

- **安全漏洞的評估** (Breach Assessment)：Threat Defense for AD 會使用攻擊模擬技術持續探測網域的不當組態、漏洞及持續性，並由攻擊者觀點向 Active Directory 管理員呈現其網域狀態，以便立即緩和風險減少攻擊面。
- **裝置控管** (Device control)：針對不同類型的裝置，例如 USB、紅外線裝置和 FireWire，可由政策阻止或允許該裝置連接到電腦，如此便可減少威脅和被滲透的風險。
- **應用程式控管** (Application Control)：透過僅允許執行已知安全的／經授權的應用程式，將端點攻擊面減至最少，進而強化對進階攻擊的防禦。
- **行為隔離**以最小的操作影響限制了受信任應用程序的異常和危險行為。
- **弱點矯正** (Vulnerability Remediation)[3]：賽門鐵克端點漏洞修復能提供漏洞及其相關風險的能見度和情報來強化安全態勢。該解決方案可發現漏洞，根據 CVSS(通用漏洞評分系統) 對嚴重程度進行排名，並確定受影響設備的數量，以確保您優先解決最關鍵的威脅。

3: 只支援 Win 10、Win 10 S Mode、 iOS 以及 Android

攻擊預防

賽門鐵克多層端點防禦可立即有效地提供保護，對抗各種檔案及無檔案攻擊媒介和方法。其中的機器學習及人工智慧，使用各種進階裝置及雲端型偵測方法，在各種裝置類型、作業系統及應用程式識別持續演進發展的威脅。攻擊將遭到即時封鎖，因此您的端點能夠維持完整性，避免各種不良影響。

- **惡意程式預防**：結合執行前檢測新的和不斷變化的威脅 (進階機器學習、沙箱可偵測隱藏在客製化封裝檔，監控並攔截可疑的行為) 以及基於特徵檔的偵測方式 (檔案以及網站的信譽分析與惡意程式掃描)。
- **刺探利用預防**：攔截記憶體型態的零日攻擊防護能力，以保護常用的應用程式和作業系統免受威脅。
- **密集型防護**：可以讓 IT 安全團隊調適偵測和攔截等級，進而最佳化防護功能，並且為每名客戶提升可疑檔案的能見度。
- **維護連線安全**：可識別惡意 Wi-Fi 連線，並利用熱點信譽技術，提供政策導向 VPN，以保護網路連線及支援合規性。

入侵預防

賽門鐵克的入侵預防，防禦攻擊者有任何機會入侵企業組織內部之前，儘早在端點處遏制攻擊者。 各種 AI 驅動的欺敵和入侵防禦技術可以協同運作，在端點入侵發生之前和入侵發生之後立即阻止進一步的攻擊，避免爆發更嚴重的全面性破壞。

- **入侵防禦和防火牆**：使用規則和政策攔截已知的網路攻擊和瀏覽器型的惡意程式攻擊，並通過自動將網域 IP 位址列入黑名單來阻止端點與命令和控制 (C&C) 的回報連線。
- **欺敵技術** (Deception)：使用誘騙和誘餌 (如假檔案、假憑證、假網路共享、假快取項目以及假端點) 的主動式安全功能，欺騙攻擊者進入而讓自己曝光與其攻擊目標，能夠揭露並延誤攻擊者的行為。
- Active Directory **安全性**：在端點結合 AI、模糊和進階鑑識方法來因應各種秘密攻擊或 APT，以提供自動入侵遏止、資安事端回應及網域安全評估等功能。這是唯一的安全解決方案，能在攻擊者入侵端點後加以遏止，不會讓攻擊者存留在網域中。本解決方案可中斷偵查活動、防止憑證竊取、避免攻擊者利用 Active Directory 橫向移動至其他資產。
- **自動化政策管理**：採用機器學習和先進人工智慧，以獨特方式結合了入侵指標 (IoC) 和歷史異常指標，不斷調整端點政策臨界值或規則，持續保持最新狀態並與組織的當前風險狀況保持一致。

入侵後的回應與矯正

賽門鐵克結合了端點偵測和回應 (EDR) 技術以及無可比擬的安全運營中心 (SOC) 分析師的專業知識，提供您需要的各種工具，迅速解決端點資安事件，並盡可能減少攻擊影響。於單一代理程式架構整合 EDR 功能，同時支援傳統與現代的端點。可以精確檢測各種進階攻擊，提供即時分析，並使您能夠主動地發現威脅並進行進行鑑識調查和補救。

- **行為分析** (Behavior Forensics)：使用者行為分析能記錄與分析端點行為來識別進階攻擊的戰術與技術，偵測偽裝成合法使用者卻執行異常活動的攻擊者。EDR 工具會依據 ATT&CK 矩陣中的戰術與技術，說明各種攻擊方法。此外，快速篩選功能可讓調查人員輕鬆將結果範圍縮小至 MITRE ATT&CK 生命週期的一或多個階段，包括初始存取、持續存在、橫向移動及指令和控制。
- Symantec EDR 提供了**進階威脅搜尋** (Advanced Threat Hunting) 工具：精準偵測各種進階攻擊，提供即時分析，協助您主動搜尋威脅，進行鑑識調查。其中內建 MITRE 網路分析等自動教戰守則，可依據 MITRE ATT&CK 模型建議調查，提升安全分析生產力，也可以在整個企業內部搜尋端點的入侵指標 (IoC)。
- **整合式回應**：賽門鐵克 EDR 可以直接對端點採取行動，迅速修復受影響的端點，包括資料擷取、檔案刪除、加入黑名單及端點隔離。可自動遞交經確認為可疑的檔案給沙箱，包含具虛擬機器感知能力的惡意程式 (也就是可躲開傳統沙箱的偵測功能)。

入侵後的回應與矯正 (接續前頁)

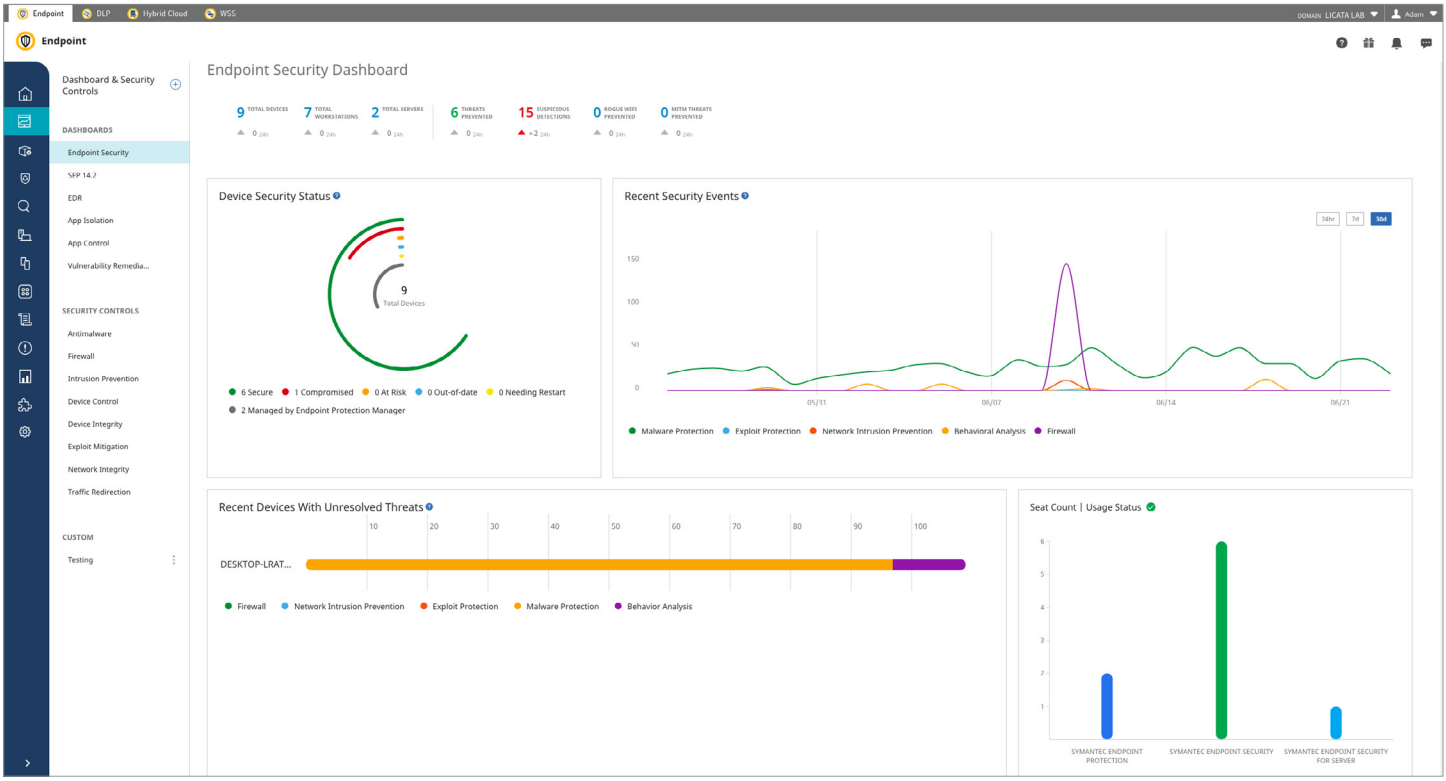
- **威脅獵人** (Threat Hunter) 搜尋高質感事件，並結合了先進的機器學習和專業的 SOC 分析人員的力量，以發現對手使用的工具、戰術和程序。它確保可以根據相關情境快速識別關鍵攻擊。此外，它還提供對 Symantec 全球安全數據的直觀訪問，以增強您團隊的威脅搜尋工作。
- **快速回應**可以把矯正威脅和即時回應攻擊者的時間降到最低。內置工具和劇本通過隔離攻擊者來遏制威脅，並提供對端點的交互式存取。

輕鬆維護動態端點環境安全

單一代理程式堆疊可減少端點安全足跡，同時整合 (及協調) 可用的最佳預防、偵測及回應、欺敵及強化技術。從單一系統實現全面管理，盡可能減少設定、實施、管理及維護安全態勢所需的時間、資源及工作。您需要的一切只要按一兩下滑鼠就可取得，協助提升管理員生產力，並加速回應時間，以迅速解決安全事件。

- **AI 引導安全管理**—更精準地更新政策，減少設定不當問題，以強化安全檢疫。
- **簡化工作流程**—確保一切都順利配合，以提升效能、效率及生產力。
- **情境感知建議**—消除例行作業，制定更妥善的決策，以達成最佳效能。
- **自主安全管理**—持續由管理員及使用者行為學習，以加強威脅評估、微調回應，並強化整體安全態勢。

圖二：管理者介面

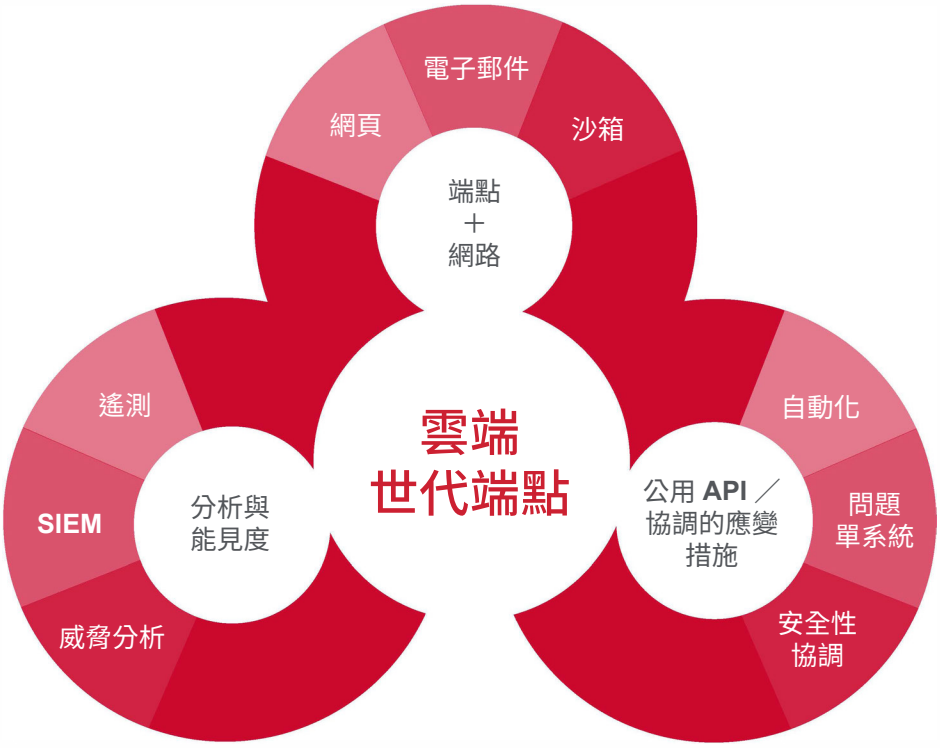


整合賽門鐵克產品組合及第三方產品來降低複雜性

SES 是一款必要的解決方案，可加快功能整合，並讓 IT 安全團隊，在任何地點偵測網路中的威脅，並透過協調回應來加以解決。SES 能夠和賽門鐵克解決方案 (例如做為整合式網路防禦平台的主要元件) 或第三方產品 (透過公用 API) 搭配使用，進而提升安全態勢。賽門鐵克整合式網路防禦平台結合雲端和內部部署的安全功能，可以保護使用者、資訊、即時訊息和網路，並由無與倫比的威脅情報提供強大支援。賽門鐵克是唯一一家提供整合式解決方案的供應商，能夠在網路閘道 (網頁和電子郵件安全閘道) 進行威脅偵測，並觸發端點協調回應 (黑名單和矯正)。目前已整合：

- **Symantec Web Security Service**：使用 PAC 檔案將 Web 流量從漫遊使用者重新導向至 WSS 及 CASB。
- **Symantec Web Gateway**：可編程的 REST API，能夠與 Secure Web Gateway 等現有安全基礎架構整合，進而在端點協調回應，快速終止感染擴散。
- **Symantec Validation and ID Protection**：多重因素驗證整合，在 SEP Manager 主控台內部支援 Symantec VIP 及 PIV/CAC 智慧卡進行驗證。
- **Symantec Content Analysis**：利用動態沙箱 (自建或雲端：實體／虛擬) 及多層式檢測引擎進一步偵測和封鎖規避傳統分析的進階威脅。
- **Symantec Data Loss Prevention**：藉由向 DLP 提供可疑應用程式的即時威脅情報，防止機敏資料外洩。

圖三：賽門鐵克端點安全 -Symantec Endpoint Security



圖四：授權選項

功能特色

	SEP	SES ENTERPRISE	SES COMPLETE
	業界端點防護的標竿。連續五年獲得最佳防護評鑑，現在更獲得 AV Test 最佳效能獎。	延伸 SEP 的防護至智慧型手機及平板等行動裝置，並同時支援雲端中央主控台控管。	提供業界最完整的端點安全，除 SEP 及 SESE 的功能外，另涵蓋 EDR、AD 防護，威脅搜尋及其它創新技術，提供無人能及的完整端點安全覆蓋面。
集中管理選項	地端自建	地端自建、原廠雲端、地端/雲端混合	
代理程式需求	單一代理程式		
支援裝置 企業擁有、員工自攜、訪客自攜	筆電、桌機、伺服主機	智慧型手機、平板裝置、筆電、桌機、伺服主機	
支援作業系統	Windows、macOS、Linux	Windows (including S Mode and Arm)、macOS、iOS、Linux、Android	

防護技術

	SEP	SES(企業版) ENTERPRISE	SES (完整版) COMPLETE
攻擊預防			
業界最強的攻擊預防	✓	✓	✓
行動裝置威脅防護		✓	✓
連線安全檢查		✓	✓
降低攻擊面 (曝險機會)			
入侵評估			✓
基於行為的威脅隔離			✓
應用程式控管			✓
裝置控管	✓	✓	✓
入侵預防 ...			
入侵預防	✓	✓	✓
用戶端防火牆	✓	✓	✓

	SEP	SES(企業版) ENTERPRISE	SES (完整版) COMPLETE
... 入侵預防			
欺敵／誘敵	✓	✓	✓
AD 安全防護			✓
回應與矯正			
端點偵測與回應			✓
目標攻擊雲端分析			✓
行為鑑識			✓
威脅搜尋			✓
快速回應			✓
IT 維運管理			
搜尋與佈署	✓	✓	✓
主機完性檢查	✓	✓	✓

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 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。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，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw