Symantec by Broadcom

解決方案簡介

重要特色

- 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：攻擊面縮小、攻擊預防、入侵預防以及偵測與回應
- 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
- 自適應防護
- 事件預測
- 保護 Active Directory
- 進階應用程式控制
- 人工智慧 (AI) 引導的安全管理
- 目標式攻擊分析與威脅搜尋
- 全球情報網路 (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

賽門鐵克端點安全解決方案
(Symantec® Endpoint Security)
自動化、客製化與最大化保護

解決方案簡介

全球企業投入大量資源於端點安全解決方案，以保護其珍貴資產。儘管耗費時間與金錢，時至今日，發生的資安事件仍持續增加。但原因何在？

有些資安解決方案為了減少誤報，會降低其保護等級。若再加上設定錯誤與安全設定薄弱，端點系統遭入侵的的原因顯而易見。

全球網路威脅比以往更具侵略性和破壞性，因此強化預防措施刻不容緩。由於現代攻擊的偵測與反應窗口持續縮短，因此在攻擊未發生之前進行預防至關重要。投資事件應變機制同樣關鍵，能建立堅實的安全態勢以防範未來攻擊。

解決之道何在？理想的端點安全解決方案需要最大限度地提高端點保護，並在所有裝置、作業系統及整個攻擊鏈中實現最大保護與效能平衡的策略。

賽門鐵克端點安全為您的組織提供客製化防護，節省時間、金錢與人力成本。採用賽門鐵克解決方案，您無需在「最佳安全性」與「最大簡易性」之間左右為難。現在，您可以「魚與熊掌」兼得。

解決方案概覽

賽門鐵克端點安全解決方案 (Symantec® Endpoint Security, SES) 為現代企業提供全面、整合的端點安全保護。多元的中央管理主控台支援自建地端部署、混合雲或原廠雲端部署。透過單一代理程式可保護所有傳統和行動裝置端點，在裝置、應用程式和網路層級提供環環相扣的防禦措施。統一的雲端中央管理主控台簡化了進階威脅的防護、偵測和回應，並運用人工智慧 (AI) 來優化安全決策。

圖一：賽門鐵克端點安全解決方案 (Symantec® Endpoint Security)

為組織提供無與倫比的端點安全

賽門鐵克端點安全 (Symantec® Endpoint Security) 提供整合式端點安全防護功能，協助您降低整體風險、預防攻擊入侵您的端點，並消弭任何已滲透的威脅。賽門鐵克端點安全提供整合式端點防護功能，協助您降低整體風險、阻擋攻擊觸及端點，並中和任何已經滲透的威脅。

賽門鐵克解決方案透過「自適應防護 (Adaptive Protection)」技術縮小攻擊面並消除盲點，此創新方法協助您提早在攻擊前就預先做好準備，聚焦於強化整個攻擊鏈的防護能力。自適應防護能自動化安全配置，無需人工操作即可為每個組織提供客製化保護。主動式攻擊面縮小與創新攻擊防禦技術，可對抗依賴隱蔽惡意軟體、憑證竊取、無檔案攻擊及內建合法工具 (living-off-the-land，就地取材攻擊) 的威脅，提供最強大的防禦。

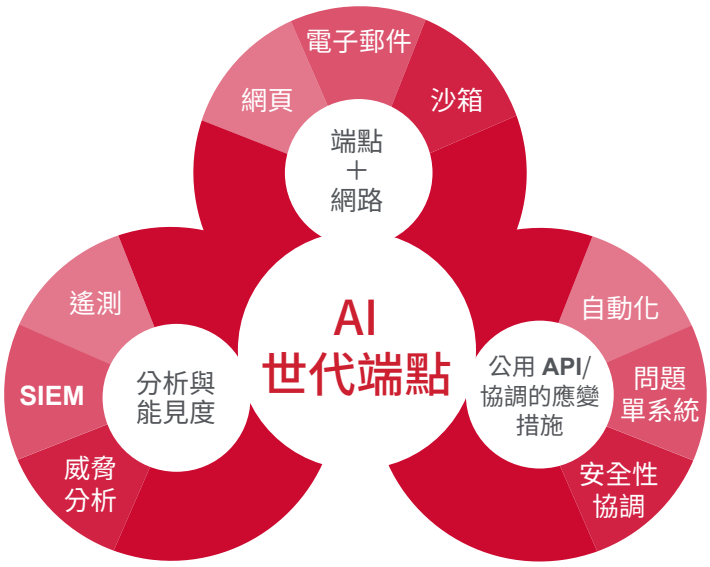
賽門鐵克解決方案更能於資料外洩前，防止全面性的入侵行為發生。透過精密攻擊分析、行為鑑識、自動化調查劇本 (Playbook)，以及業界首創的橫向移動與憑證竊取防禦機制，可提供精確的攻擊偵測與主動式威脅獵捕，即時封鎖攻擊者並解決持續性威脅。

攻擊面縮小

賽門鐵克解決方案能夠透過針對各種不同環境客製化強制執行的「縮小攻擊面」功能，並運用進階策略控制機制實施執行，協助您主動強化資安態勢。藉由持續掃描應用程式、Active Directory 及裝置中的漏洞與錯誤配置之技術，可大幅縮小攻擊面，消除諸多攻擊戰術和技術對端點資產構成的風險。

- **自適應防護 (Adaptive Protection)**：會監控您的環境，尋找基於正當業務理由極少使用或從不使用的應用程式和行為。它會封鎖或或限制對這些應用程式的存取權限，防止攻擊者藉此發動攻擊或潛伏於環境中。
- **安全漏洞評估 (Breach Assessment)**：AD 威脅防禦會透過攻擊模擬技術持續探測 Active Directory 中的網域錯誤配置、漏洞及持久性問題，協助管理員能即時識別風險並提供緩解與修復建議。
- **裝置控管 (Device control)**：針對連接至用戶端電腦的各類裝置，例如：USB、紅外線和 FireWire 裝置，可由政策設定阻斷或允許策略，降低威脅與資料外洩風險。
- **應用程式控管 (Application Control)**：評估應用程式風險與漏洞，僅允許已知安全的／經授權的應用程式執行。

圖二：賽門鐵克端點安全--Symantec® Endpoint Security



攻擊預防

賽門鐵克多層次攻擊預防能即時有效抵禦基於檔案與無檔案的攻擊途徑及手法。透過結合機器學習 (ML) 與人工智慧 (AI)，並運用進階的裝置端與雲端偵測機制，賽門鐵克解決方案可跨裝置類型、作業系統及應用程式識別不斷演變的威脅。攻擊會即時遭到封鎖，因此您的端點能夠維持完整性，避免各種不良影響。

- **惡意軟體防護**：結合執行前偵測與攔截機制，及特徵碼 (簽名) 的偵測方法，用以識別並緩解惡意軟體威脅。執行前偵測方法利用先進的機器學習 (ML) 和沙箱技術，可偵測隱藏於自訂封包中的惡意軟體。透過行為監控與可疑檔案阻斷機制，能有效應對新興與持續演變的威脅。基於簽名／特徵碼的防護方法包含檔案與網站信譽分析及惡意軟體掃描，可精準識別並緩解惡意軟體風險。
- **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漏洞攻擊威脅。
- **事件預測**：結合人工智慧的強大能力與對超過 50 萬個真實世界攻擊鏈的分析相結合，能以高達 100% 的確定性預測攻擊者接下來的四到五個動作。
- **密集型防護**：可以讓 IT 安全團隊透過精細調整偵測與封鎖程度，優化對可疑檔案的防護效能，提升可疑檔案的可視性。此功能使用先進的機器學習技術，針對可能有害的檔案提供更積極的偵測。
- **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

賽門鐵克的防禦策略是攻擊者有機會在網路上常駐之前，儘早遏制攻擊者，使其無從在網路中建立持久存在。多項由人工智慧驅動的誘騙技術與入侵防禦系統協同運作，在端點受到入侵之前和緊隨其後，即全面性入侵發生之前，便能阻斷攻擊者的網路持久化企圖。

- **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)**：運用誘騙和誘餌 (例如：偽造檔案、假憑證、假網路共享、假快取項目、網頁請求以及假端點) 的主動式安全功能，藉此揭露攻擊者身分、判斷其意圖與戰術，並延緩其預定攻擊行動。
- **Active Directory 安全機制**：透過無限混淆技術，控制攻擊者對組織 Active Directory 資源的感知，從而抵禦橫向移動攻擊與網域管理員憑證被盜等主要攻擊面威脅。在這種「無限混淆」的策略下，攻擊者將因與虛假資產互動或嘗試使用無效的網域管理員憑證而暴露自己的行蹤。
- **自動化政策管理**：採用先進人工智慧和機器學習，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。
- **事件預測 (Incident prediction) 功能**：會根據過去的攻擊模式，自動識別特定攻擊者接下來可能採取的步驟。隨後系統將執行緩解策略阻斷這些預測中的攻擊行為，在攻擊者加密或外洩資料之前，便能中斷大多數攻擊者的進展。

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，以及其無與倫比的資訊安全營運中心 (SOC) 分析師專業知識，簡化端點調查與回應工作流程，並將攻擊影響降至最低。透過同一套保護傳統與現代端點的代理程式及中央管理主控台，賽門鐵克 EDR 可精確偵測進階攻擊、提供即時分析，並讓您能夠進行鑑識調查和修復。

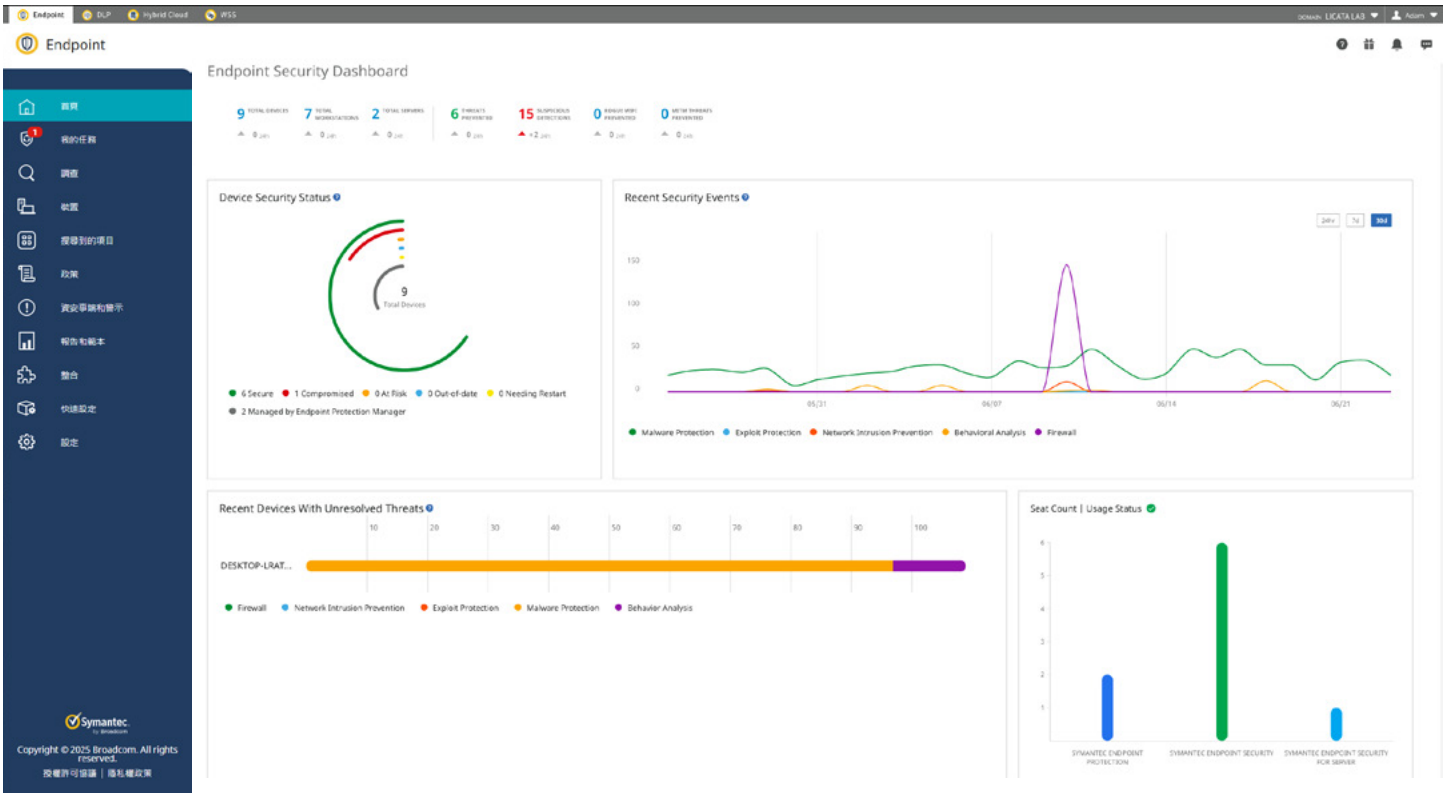
- **行為鑑識 (Behavior forensics)** 技術透過記錄與分析端點行為，識別可能利用合法應用程式進行惡意活動的高階攻擊手法。此數據結合 MITRE ATT&CK 框架，轉化為更完整、更有洞察力的資訊資產。協助引導事件應變人員在調查期間進行分析、掌握關鍵指引。
- **進階威脅搜獵 (threat hunting)** 工具可橫跨記錄事件的中繼資料進行搜尋，並識別特定時間點的端點狀態。事件應變人員亦能透過直接查詢端點，在企業範圍內搜尋入侵指標 (IOCs)，透過搜尋網路中可能規避自動偵測的複雜威脅，來改善組織的安全態勢。
- **整合式回應**：透過在端點執行直接行動進行修復，包括檢索檔案、刪除檔案、隔離端點及封鎖存取。賽門鐵克端點安全解決方案會自動將可疑檔案提交至沙箱進行完整惡意軟體分析，其中包含偵測具備虛擬機器感知能力的惡意軟體 (也就是可躲開傳統沙箱的偵測功能)。
- **威脅獵尋能力**有助於識別識別高擬真度事件，並揭露攻擊者使用的工具、戰術與程序 (TTPs)，確保關鍵攻擊能迅速被識別並優先處理對組織特定環境最具威脅性的攻擊。此外，透過存取賽門鐵克全球安全數據，您的團隊能獲得對實際攻擊事件的洞察，從而強化威脅獵捕工作。
- **事件分析功能**可識別潛在可疑活動，並自動將相關事件關聯成單一事件以供調查，讓分析人員或安全團隊能夠集中精力進行後續追蹤和處理。
- **自適應事件**會標記可疑行為的異常來源，並將這些行為彙整為單一事件，您只需透過簡單調整您的『適應性保護』政策來解決。

輕鬆保護您的動態端點環境

單一代理程式的端點安全透過整合與協調最佳可用的預防、偵測及回應技術，讓代理程式保持輕量並優化效能。透過單一雲端管理系統統籌所有作業，可大幅降低配置、部署、管理及維護安全態勢所需的時間、資源與人力成本。您所需的必要功能僅需點擊一兩下即可存取，不僅提升管理員工作效率，更能加速應對時效，迅速解決資安事件。

- 安全性政策調整**自動化**，以更符合您獨特環境的安全需求。
- **簡化**工作流程以提升效能、效率與生產力。
- 透過情境感知建議，消除例行手動任務，從而**優化**效能。
- 運用自主安全性管理持續學習管理員與使用者行為，以優化威脅評估、調整回應措施，並**強化**您的整體安全性態勢。

圖三：賽門鐵克端點安全(SES)管理介面



賽門鐵克透過其整合式產品組合及與第三方解決方案的協作，協助企業降低資訊安全環境的複雜性，同時提升安全態勢與營運效率

作為端點安全的核心解決方案，賽門鐵克端點安全防護 (Symantec® Endpoint Security) 可與其他賽門鐵克解決方案搭配使用，並透過專用應用程式和發布的 API 與第三方產品協作，共同強化您的安全態勢。沒有其他供應商能提供如此完善的整合式解決方案，可隨時隨地在您的網路中偵測威脅，並在網路和電子郵件安全閘道偵測到威脅時，即刻在端點觸發回應機制。

具體整合功能如下：

賽門鐵克雲端網頁安全閘道服務 (Symantec Cloud SWG)

透過全通道重定向或 PAC 檔案，將漫遊賽門鐵克端點安全用戶的網路流量導向賽門鐵克雲端網頁安全閘道服務 (SWG) 及賽門鐵克雲端存取安全平台 (CASB)。全通道重定向會將所有網路流量導向，而 PAC 檔案則提供更精細的控制，僅針對特定流量進行重定向。

賽門鐵克驗證與身分保護 (Symantec Validation and ID Protection)

支援包含個人身分驗證卡 (PIV) ／通用存取卡 (CAC) 在內的多因素驗證，適用於賽門鐵克端點安全本地部署環境。

賽門鐵克內容分析系統 (CAS-Symantec Content Analysis)

賽門鐵克內容分析 (CAS) 會自動將潛在零時差威脅升級並轉交處理，在將內容傳送給使用者前進行動態沙箱檢測與驗證。透過單一中央位置分析未知內容。此惡意軟體分析器運用 Edge Secure Web Gateway，採用獨特的多層次威脅檢測引擎與動態雙重沙箱技術，揭露惡意行為並暴露零時差威脅，同時安全引爆可疑檔案與網址。可將入侵指標 (IoCs) 傳送至端點偵測技術，整合終端用戶端點安全防護。

賽門鐵克資料外洩防護 (DLP)

透過向 DLP 提供可疑應用程式的即時威脅情報，防止敏感資訊外洩。DLP 是企業面臨目標式網路攻擊、數位轉型及隱私法規等數資料保護挑戰值得優先導入的方案。

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

攻擊預防	SEP	SES(企業版) ENTERPRISE	SES(完整版) COMPLETE
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	✓	✓	✓
欺敵／誘敵	✓	✓	✓

入侵預防	SEP	SES(企業版) ENTERPRISE	SES(完整版) COMPLETE
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			✓
自適應防護			✓
行為鑑識			✓
威脅搜尋			✓
威脅情資			✓
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