Symantec Endpoint Security
賽門鐵克端點安全 三種不同料號比較表

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 (包含 S Mode & Arm)、macOS、iOS、Linux、Android	

防護技術

攻擊預防	SEP	SES ENTERPRISE	SES COMPLETE
業界最強的防惡意軟體技術 以機器學習為後盾	✓	✓	✓
	提供多層次的防護技術，包括： ✓ 防惡意程式 ✓ 惡意行為預防 ✓ 密集型防護 ✓ 進階機器學習 ✓ 記憶體攻擊緩和		
行動裝置威脅防護		✓	✓
	協助預測、偵測和預防實體、惡意軟體、網路和漏洞利用，保護業務免於行動裝置網路攻擊。		
連線安全檢查		✓	✓
	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。		

攻擊面降低

入侵評估

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。

基於行為的威脅隔離

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。

應用程式控管

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。

裝置控管

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。

入侵預防

入侵預防

採用最新的深層封包檢測技術，分析所有內送流量和外寄流量並提供瀏覽器防護，以及連線至惡意的C&C主機，以便此類威脅在電腦上執行之前予以攔截。

用戶端防火牆

使用預設或自訂的用戶端防火牆政策來管理網路存取。

欺敵／誘敵

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。

AD 安全防護

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。

回應與矯正

端點偵測與回應

		✓

提供可採取行動的精闢見解情資、行為鑑識和先進的調查與回應工具為您的SOC提供支援，擴充您的 SOC 團隊的戰力。

目標攻擊雲端分析

		✓

從所有Symantec端點用戶的遙測資訊中應用機器學習，可以檢測出全新的攻擊並提供建議的操作。

行為鑑識

		✓

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。

威脅搜尋

		✓

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)。

快速回應

		✓

迅速修正端點，確保威脅不會再次入侵

IT 維運管理

搜尋與佈署

✓	✓	✓

在滿足系統需求的前提下，可透過網路掃描發現未受控管的裝置，並從遠端安裝及管控。

主機完性檢查

✓	✓	✓

主機完整性可確保用戶端電腦受到防護並遵從公司的安全性政策。主機完整性政策可用於定義、強制執行和還原用戶端的安全性，以保護企業網路和資料的安全。

Symantec™
A Division of Broadcom

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政策性整合式解決方案，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

本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2021/05/01