

SEP與SES之間的自適應防護功能比較

最新更新日期：2025 年 2 月 14 日

下表顯示從下列項目管理用戶端時的自適應防護功能差異：內部部署 Symantec Endpoint Protection Manager、具有輕度註冊的 Symantec Endpoint Protection Manager 或混合管理 (在雲端中註冊 Symantec Endpoint Protection Manager)。

內部部署和輕度註冊選項使用 Symantec Endpoint Protection Manager 自適應防護政策。混合管理使用 Symantec Endpoint Security 雲端伺服器中的自適應防護政策。

	內部部署	具有輕度註冊的內部部署	混合/SES
熱圖普及率和事件計數 提供根據參與者和目標的行為感染狀況二維視覺化。此雙重維度檢視可更深入地了解如何在環境中傳播行為。 調適型防護如何收集感染狀況和事件計數？	是*	是*	是
快速調整 攔截所有零感染狀況行為。您有機會在攔截發生之前將其核准。	是	否	是
自動調整 自動識別並拒絕特定行為，以協助減少攻擊面。	否	否	是
威脅態勢鑑識 顯示全域威脅態勢中的最近攻擊，以及應用程式行為可能發生的攻擊鏈。	否	否	是
遙測指示器 顯示警示列或圖示以反白顯示遙測問題，以及指向疑難排解步驟或診斷工具的連結。	否	否	是
大量變更 可讓您選取多個行為，並且一次予以套用。	否	否	是
政策建議 提供建議，而建議是根據賽門鐵克對您環境內行為的歷史分析。這些見解使用遙測資料和威脅情報來判斷可以安全攔截的內容。	否	否	是

	內部部署	具有輕度註冊的內部部署	混合/SES
政策管理 可讓您選取要套用熱圖的政策。熱圖資料是從使用此政策的所有電腦所收集。	是	否	是
例外管理 可讓您修改現有規則以允許在客戶環境中觀察到的特定合法行為，同時仍然強制攔截相同行為的一般實例。	否	否	是

*在 Symantec Endpoint Protection Manager 中，切換顯示 30、60 或 90 天，而不是 90、180 或 365 天。

輕度註冊提供在 Symantec Endpoint Protection Manager 中管理自適應防護的最佳結果。輕度註冊會將 Symantec Endpoint Protection Manager 所管理的電腦中的遙測資料與 Symantec 後端遙測資料庫中的資料進行比對。管理伺服器必須提交遙測，自適應防護才能取得感染狀況。

如果您註冊到雲端，則雲端中的自適應防護政策會覆寫您在 Symantec Endpoint Protection Manager 中所新增的政策。

輕度註冊如何運作？

輕度註冊是在 LiveUpdate 第一次將調適型防護內容下載至 Symantec Endpoint Protection Manager 時發生的背景程序。輕度註冊的目的是讓 Symantec Endpoint Protection Manager 建立一種與 Symantec Endpoint Security 雲端伺服器通訊以及接收資料的方法。輕度註冊還會將您的 Symantec Endpoint Security Complete 授權與您公司中的資料比對。

輕度註冊的工作方式如下：

- LiveUpdate 會將內容下載到 Symantec Endpoint Protection Manager，這會啟動向雲端伺服器的註冊工作。此註冊工作：
 - 驗證 Symantec Endpoint Security Complete 授權。
 - 檢查 Symantec Endpoint Protection Manager 網域中的用戶端群組是否已啟用遙測。如果大部分用戶端裝置硬體金鑰 (MID) 相符，則適當的 API 會向雲端伺服器傳回回應，指出您的組織符合註冊條件。
- 雲端伺服器授權註冊。

如果註冊失敗，則「進階安全性」頁面會顯示 401 錯誤。如果已註冊 SEPM 網域，則您會看到 403 錯誤。

請參閱「進階安全性」頁面問題疑難排解。



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)

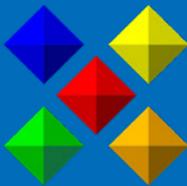


Symantec
A Division of Broadcom

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。



保安資訊
KEEPSAFE
INFORMATION SECURITY

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, 以及基於比原廠更熟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、可以提供良好諮詢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。