三種端點安全解決方案，滿足不同預算、環境與情境以及最高等級的安全要求

企業內部端點裝置的數量龐大，平台及版本也常不同，遠離企業防火牆保護的行動裝置，更是與日俱增。所以要維持一個穩健的端點安全防護環境，相當費力(像是作業系統、應用程式的修補程式有無更新至新、病毒定義檔是否有更新、是否有安裝了非必要的軟體…)。端點更是攻擊者虎視眈眈的主要目標，因為端點能連接至企業內部重要系統、存取寶貴的資料。就防護機制而言，也只有端點特有的環境與條件，才能完全符合惡意程式被觸發的條件，再加上「人」的無心或有意的人性漏洞，才能觸發所有惡意程式。根據Verizon資料外洩調查報告顯示，23%的員工可能打開網路釣魚電子郵件，11%的員工會打開來自未知人員的附件。同時資料外洩調查報告，也顯示，在整年度的所有網路間諜活動中，惡意軟體被利用率高達90%，不管是經由電子郵件、網頁順道下載、直接或遠端安裝。所以，企業部署了防火牆、入侵預防、網頁安全與過濾、郵件安全與過濾、垃圾郵件防護，還是無法完全根除端點上的威脅。利用惡意程式的網路釣魚、網頁攻擊、隨身碟交互感染等基於人性的社交工程攻擊，除了務實地持續進行教育訓練與考核外，端點防護作為資安的最後關卡，更是至關重要。

賽門鐵克的端點安全軟體有三個版本，可以滿足不同預算、環境與情境以及最高等級的端點安全要求：

- SEP(Symantec Endpoint Protection)--賽門鐵克**端點防護**
- SESC(Symantec Endpoint Security Complete)--賽門鐵克**端點安全完整版**
- SESE(Symantec Endpoint Security EnterPrise)--賽門鐵克**端點安全企業版**

SESC(Symantec Endpoint Security Complete)--賽門鐵克端點安全完整版--完整版就是包括整個攻擊鏈的生命週期所需的對應防護功能都有的意思。不管從NIST所規範的五階段的框架，還是拆解洛克西德馬丁公司所註冊的**網路攻擊鏈七步驟**，SESC總能在攻擊前、攻擊中、入侵中以及入侵後提供最佳的預防、保護以及回應。

在台灣大家熟悉的賽門鐵克端點防護：**SEP**(Symantec Endpoint Protection)，算是最必要的基本防護，它的中央管理主控台(**SEPM**)是安裝在地端自建的Windows伺服主機，可以支援**Windows/Macintosh/Linux**三種用戶端平台。

近5年來，由於行動裝置及遠端辦公越來越多，所以**Android/IOS**的安全需求也跟windows平台要求一樣高，所以就有了**SESE**(Symantec Endpoint Security Enterprise)--賽門鐵克端點安全企業版這個料號，這個料號同時支援地端/原廠雲端的中央管理主控台(SEPM)，也比SEP多支援Android/IOS等主流行動平台。

SESC(Symantec Endpoint Security Complete)--賽門鐵克端點安全完整版--它有SEP及SESE的所有功能。另還包含**EDR**(端點偵測與回應)以及**AD防護**的功能。近期頻傳的大企業遭受加密勒索或索贖款不成將公告其機敏資

料的商業集團式或國家支持的駭客組織，讓許多人有一種防不勝防的無力感，其實是大部份的單位，只專注在預防上，所以被入侵之後，完全束手無策，也沒有機制可以查找可疑或非法的行為，這種被入侵之後的初期的預警機制、中期的肆無忌憚的橫向移動的攔截甚至是對外的惡意連線行為的阻止，如果能透過EDR及AD防護是非常有成效的，也能讓安全人員快速釐清事件的始末，不再是海底撈針。EDR透過專利的雲端沙箱及大數據的交叉比對、關聯分析的類SIEM機制，可以比SEP/SESE更高的偵測力，另外可以發現及掌控企業內部更完整的安全態勢。AD防護是利用每台用戶端的欺敵/誘餌/混淆技術，讓所有的用戶端一起協防AD核心架構，對於AD被第一時間入侵後的橫向移動行為的發現，非常利害。

上述只是主要功能的大致說明，建議參考以下的型錄連結，獲得更詳盡的資訊，如有業務及技術諮詢，歡迎來電洽詢，保安資訊將竭誠為您服務。

- **賽門鐵克端點安全完整版中文型錄**
  --Symantec Endpoint Security Complete
- **賽門鐵克端點防護企業版中文型錄**
  --Symantec Endpoint Protection
- **賽門鐵克端點偵測與回應中文型錄**
  --Symantec Endpoint Detection & Response
- **賽門鐵克端點威脅AD防護中文型錄**
  --Symantec Endpoint Threat Defense for Active Directory
- **賽門鐵克行動裝置防護中文型錄**
  --Symantec Endpoint Protection Mobile
- **白皮書：10種常見的AD配置錯誤現象**
- **SEP/SESE/SESC三個料號，功能比較表**
- **賽門鐵克端點防護獲獎無數，並深獲業界認可**

完善的資安防機制必須透過電子郵件、網頁以及端點這三個控制點的分工與協同運作，以該控制點最有利的防護技術與管理機制來降低威脅的探勘、攻擊以及入侵，並能隨時監控內部是否已被入侵及埋伏甚至橫向移動以及資料的外洩，採用Symantec完整解決方案，可以非常容易達成資安目標。現在大家都有在端點安裝防毒軟體或更強大的端點安全系統，但上報的資安事件還是層出不窮，連人才濟濟、資源豐富的大企業也不例外。其實是大部份的單位，只專注在預防上，所以被入侵之後，完全束手無策，也沒有機制可以查找可疑或非法的行為，這種被入侵之後的初期的預警機制、中期的肆無忌憚的橫向移動的攔截甚至是對外的惡意連線行為的阻止，如果能透過EDR及AD防護是非常有成效的，也能讓安全人員快速釐清事件的始末，不再是海底撈針。EDR透過專利的雲端沙箱及大數據的交叉比對、關聯分析的類SIEM機制，可以比防毒軟體或端點防護軟體更高的偵測力，另外可以發現及掌控企業內部更完整的安全態勢。AD防護是利用每台用戶端的欺敵/誘餌/混淆技術，讓所有的用戶端一起協防AD核心架構，對於AD被第一時間入侵後的橫向移動行為的發現，非常厲害。

Symantec在端點、電子郵件以及網頁防護，皆有最完整的防護機制，同時也能在這三個控制點，透過AI為後盾的關聯分析與情資交叉比對的協同運作，能在第一時間就發現目標式攻擊，更能發現入侵後的初期入侵跡象、中期橫向移動以及後期的資料外洩及更大的危害，都能有效偵測。在2019/11，博通併購賽門鐵克後，更加重投入資源在RD上，同時也大大降低交易複雜性，將料號精簡為功能多合一、實體與虛擬、地端與雲端等符合全功能多情境--並以極具競爭力的價格來提供，讓顧客更喜歡、更容易使用/採購賽門鐵克。

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)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有IT Team的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入Symantec解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊：
  保安資訊有限公司
  http://www.savetime.com.tw
  0800-381500、0936-285588