Symantec Endpoint 在 2020 MITER Engenuity ATT & CK® 評比中大放異彩

亞當·布羅姆維奇
（Adam Bromwich）
Broadcom Inc. Symantec Endpoint Security部門副總裁兼總經理

發現入侵很重要，但防止入侵更是關鍵

賽門鐵克最新的防護(Prevention)和偵測(Detection)的創新技術，在高手如林的**MITRE Engenuity的ATT&CK Evaluations最新一期的專業測試評估中**，大放異彩。此次主要針對29家廠商安全解決方案進行模擬測試，包含了174個偵測測試項目(主要測試針對進行中的攻擊及其攻擊技術的可見性和警覺性)及10個防護測試項目(測試資安解決方案在早期階段阻止惡意攻擊的防護能力)，這是首次針對資安解決方案進行偵測(detection)測試及防護(prevention)測試。結果顯示，賽門鐵克端點安全完整版(SESC-Symantec Endpoint Security)具有最強大的制敵機先的預防能力以及偵測反制能力，可為用戶提供最好的保護。

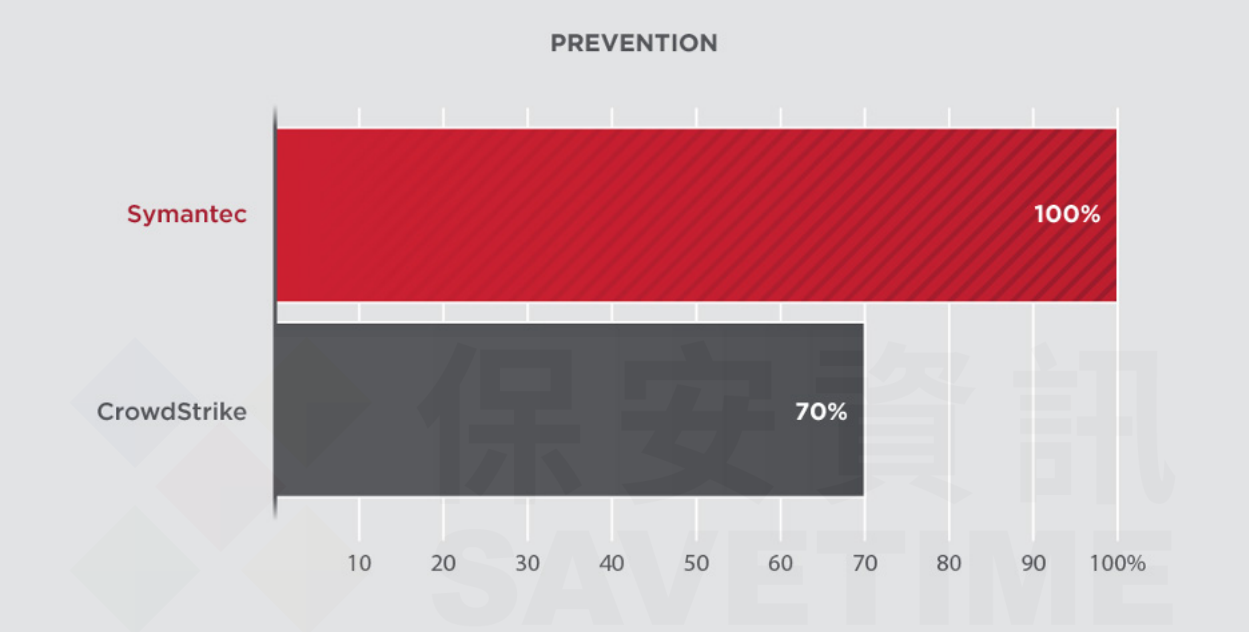
MITRE Engenuity的ATT&CK Evaluations專門測試評估資安解決方案是否具備各種已知目標式攻擊的偵測及防護能力。為了貼近真實世界常見的攻擊案例，針對以知名駭客團體**Carbanak和FIN7**的攻擊手法進行模擬測試。賽門鐵克**在所有防護(Prevention)測試中均**得分**為100%**，**在所有偵測(Detection)測試中均**得分**為91%**。賽門鐵克不僅是防護方面公認的領導者，而且其他受測廠商也無法達到像賽門鐵克如此高積分的防護和偵測完美組合。

> 結果顯示，在保護用戶方面，賽門鐵克端點安全完整版(SESC)具有壓制攻擊者的優勢反制能力。

在賽門鐵克併入成為全球最大IC公司--博通(Broadcom)的企業安全部門後，我們持續專注於防護(Prevention)以便在第一時間就阻止威脅。同時，我們也增加並強化偵測(Detection)技術來增加另一層的安全，以便找到最複雜的進階威脅。如果沒有這種平衡，安全監控中心(Security Operations Center-SOC)就會不知所措，無法發動事件和警報，攻擊者最終將會成功。事實上，大量告警似乎造成了一場行業危機，這場危機使SOC崩潰，並使他們無法專注於實際為偵測產品而設計的關鍵事件。

簡言之，發現入侵行為至關重要。但是，防止入侵(的優先順序)往往更重要--特別是讓SOC團隊的效率提升並讓它們能專注在更重要的任務上面。ATT＆CK評估結果表明，一些供應商將客戶置於過度依賴偵測(detection)而不是防護(prevention)的**困難而昂貴的**境地。(賽門鐵克的概念有點類似，普通的問題先用常識處理，特殊的問題再用專業處理，這樣專業的效益才能真正發揮，問題也能最快獲得解決。)

一些競爭者聲稱他們解決方案的防護(prevention)能力與領導品牌的一樣，但事實並非如此。

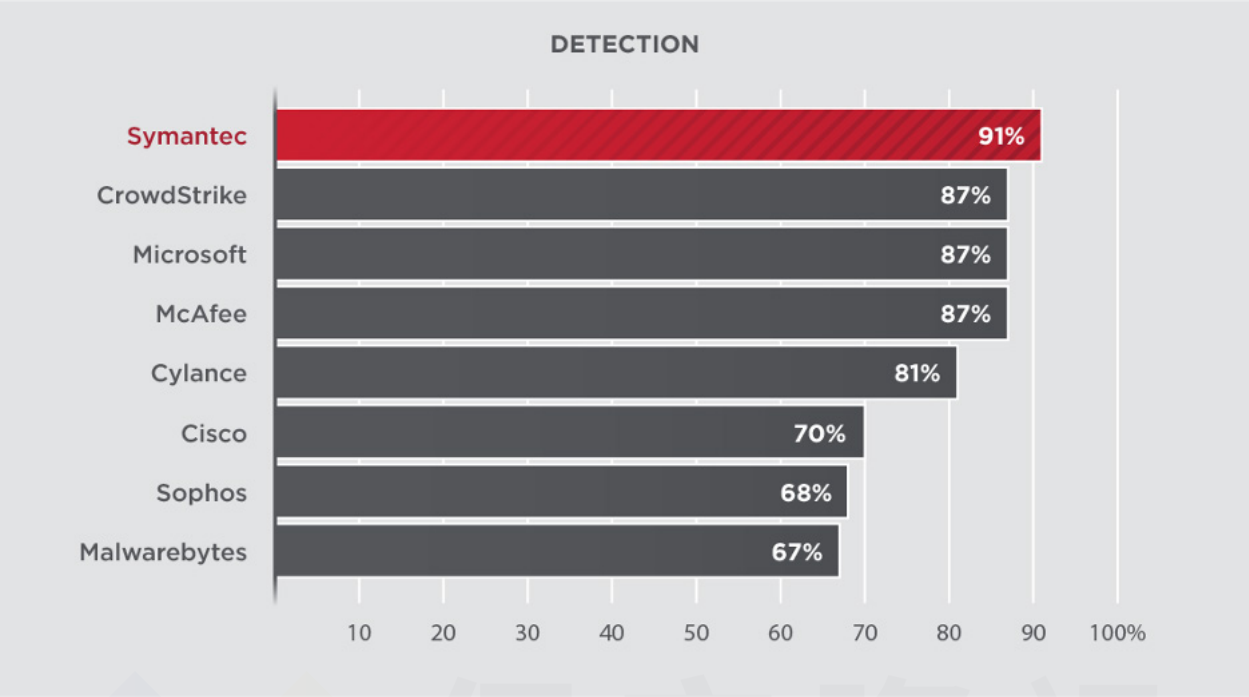


例如：賽門鐵克的端點安全解決方案提供了強大的威脅阻止功能，而其他解決方案（例如CrowdStrike）的測試結果形同聊勝於無。**SESC**內建了一系列的必要及創新技術，這些技術可提供主動的攻擊面減少功能和創新的攻擊防禦技術，可對最難偵測到的威脅提供最強大的防禦，尤其是那些頑強的隱膩惡意程式、憑證盜竊、無檔案以及“就地取材”的攻擊方法。這些強大的技術包括：

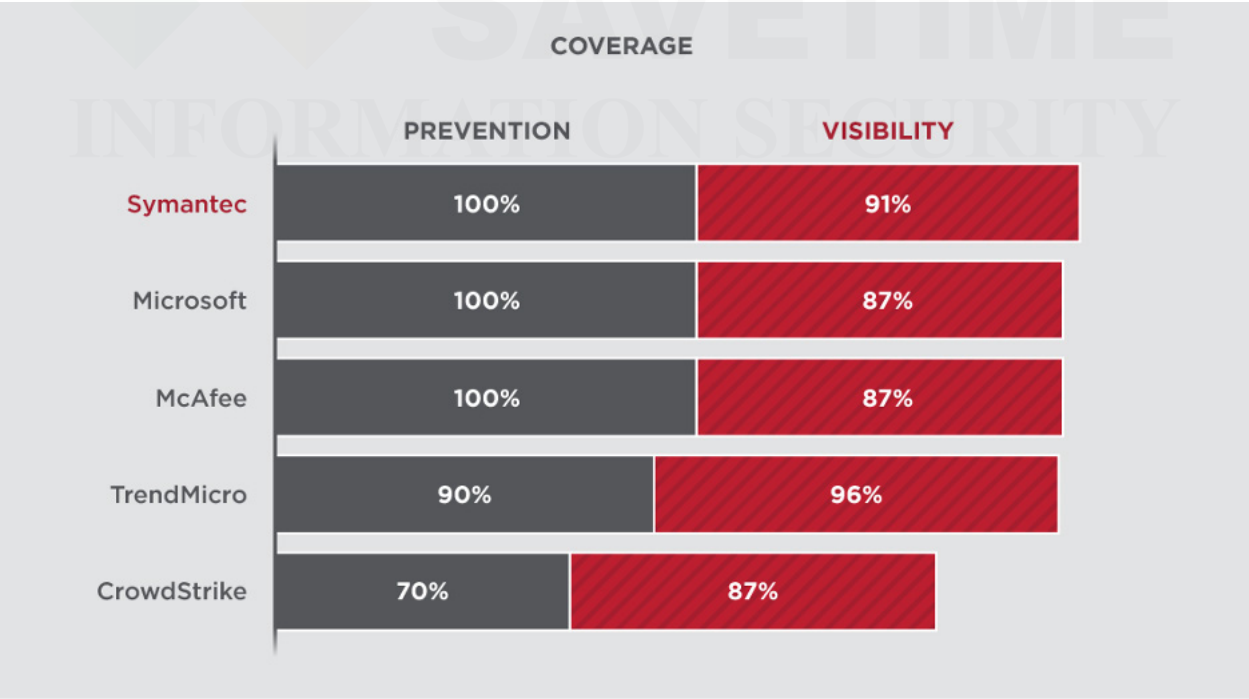
- **進階機器學習與人工智慧**--使用各種進階裝置及雲端型偵測方法，在各種裝置類型、作業系統及應用程式識別持續演進發展的威脅。攻擊將遭到即時封鎖，因此您的端點能夠維持完整性，避免各種不良影響。
- **進階刺探利用預防**--結合沙箱以及檔案行為監控技術以及攔截記憶體型態的零日攻擊防護能力，以保護常用的應用程式和作業系統免受威脅。
- **基於行為的威脅隔離**--行為隔離以最小的操作影響限制了受信任應用程序的異常和危險行為，避免正常軟體被移作攻擊工具使用。

這些技術不是客戶永遠不會啟用的選項，它們目前正在保護超過1億個企業用戶的端點。

有些廠商商聲稱他們在偵測(detection)方面也具有最高等級的地位。但這並沒有在測試中得到證明。在賽門鐵克的主要競爭對手中，SESC 在偵測方面的可見度得分最高。



ATT&CK評估結果表明賽門鐵克-最近對SESC的加重投資，已經為我們的客戶帶來實質的效益。通過添加諸如**行為隔離**之類的新技術，SESC已經證明，擴展防護(prevention)和偵測(detection)技術對於贏得與攻擊者的戰鬥至關重要。以下這張圖說明了一切：



賽門鐵克認為，客戶在選擇端點安全軟體時，無須在出色的防護(prevention)和出色的偵測(detection)之間有所取捨。因為 SESC同時都有最好的表現。

原廠網址:https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-endpoint-shines-2020-mitre-engenuity-attck-evaluations

本次Symantec參與評估產品為Symantec Endpoint Security (SES)Complete安全解決方案，相關參考資訊請參考：

- **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**

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