保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克進階機器學習技術阻擋零時差攻擊

2025 年 12 月 9 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

賽門鐵克如何運用先進機器學習技術抵禦零時差威脅

機器學習 (常簡稱 ML) 是一種非特徵碼偵測技術，能在執行前階段阻擋新型惡意軟體變種。在博通，我們於多個階層部署機器學習技術，為客戶築起抵禦網路威脅的防線。這些防護層級經精心設計，能主動與被動雙軌並行，在產品偵測到可疑檔案、作業系統事件、登錄檔項目、網址或網路活動時，立即在端點裝置、閘道設備及後端分析平台等各層級實施「攔截」。賽門鐵克憑藉全面的威脅掃描引擎，可即時動態分析新出現的內容，並將資料匯入賽門鐵克全球情報網路 (GIN)。賽門鐵克運用數百萬終端的安全遙測資料、第三方安全廠商提供的威脅相關資料源，以及豐富的乾淨檔案庫，用以訓練與評估各類機器學習模型。這些模型部署於眾多產品中，無論是在客戶端作為代理程式的一部分，或在後端分析系統中，皆能有效偵測威脅。

零時差防護至關重要

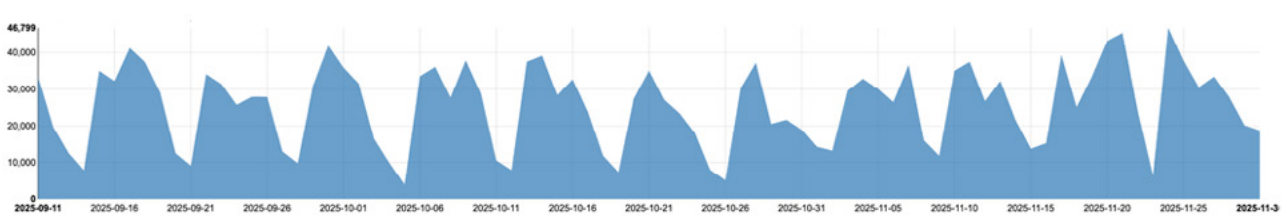
除上述分析平台外，我們還運用雲端沙箱分析引擎 (恰如其名「Cynic」)，透過運行多重機器學習模型與分類演算法，依據威脅類型、風險潛力、動態與靜態元資料及行為模式對檔案進行有效分類。賽門鐵克透過自動化系統與惡意軟體分析師，以最快速度分析客戶提交的樣本，並將情資回饋至機器學習訓練模型以提升分類效能。我們的多模型進階機器學習技術可處理各類檔案類型，並同時運行於 32 位元與 64 位元環境，提供可執行的分析結果。當偵測到防護漏洞時，後端機器學習模型將立即進行分析，並透過信譽查詢機制即時封鎖威脅。賽門鐵克進階機器學習的核心目標在於抵禦新型未知惡意軟體--業界通稱的零時差攻擊。這正是機器學習技術最能發揮優勢之處。

在過去一季中，賽門鐵克的先進機器學習技術在賽門鐵克端點與閘道產品上攔截了超過 2,060 萬次威脅。其中約 300 萬次攔截針對的是零時差攻擊--亦即任何我們的安全產品或防護技術從未遇見過的攻擊類型。這正是所謂「主動式」防護的意義所在，相較於「被動式」防護僅能在攻擊發生後新增或更新防護措施。主動防護是對抗網路威脅的靈丹妙藥，更是全球潛在網路犯罪分子的剋星。

賽門鐵克進階機器學習技術於上季提供的防護詳情：

- 網路閘道產品阻擋 1,870 萬次威脅
- 終端設備阻擋 194 萬次威脅
- 阻擋 300 萬次零時差威脅，包含：
  - 11,100 次勒索軟體 (Cerber、Gandcrab、Ryuk、Wannacry、Zombie、Cryptolocker、Lockbit 等)
  - 85.7 萬次資訊竊取者 (bancos、gamepass、lokibot、lineage、lemir、onlinegame、rultazo)
  - 1.15 萬次木馬程式 (Emotet、Nancrat、Zbot、Formbook、Killav、AsyncRAT、Remcos、trickybot 等)
  - 52.4K Win32 病毒 (Virut、Ircbot、Cridex、Extrat、Qakbot、Neshuta、Xpiro、Cridex 等)
  - 214.8K 後門程式 (Ratenjay、Zegost、Cycbot、Rifelku、Matsnu、Ghostnet、Cobalt、Breut 等)
- 392K 來自外部來源 (例如：USB 裝置與網址) 的威脅遭攔截
- 401K 基於瀏覽器的威脅於終端設備遭攔截，其中 50% 來自 Chromium 瀏覽器、31% 來自 MSEdge、5% 來自 Firefox
- 3.2K 透過命令列啟動的惡意檔案下載與執行威脅於終端產品遭攔截
- 360 萬次利用 SMB 網路檔案共享的攻擊遭攔截
- 攔截 15,000 次透過點對點網路 (例如：Anydesk (RDP)、Utorrent及BitTorrent) 下載的威脅
- 攔截 5,300 次透過腳本主機 (PowerShell／cscript／wscript) 下載的威脅

本季度於端點與閘道器上啟用零時差防護功能



欲深入了解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲深入了解賽門鐵克雲端沙箱分析引擎 (Cynic)，請點擊此處。

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-symantec-advanced-machine-learning-blocks-zero-day-attacks

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。

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。

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，以及基於比原廠更孰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、可以提供良好諮商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**。