



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

賽門鐵克檔案信譽系統

2024年8月27日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

賽門鐵克檔案信譽系統

賽門鐵克檔案信譽系統 (Symantec File Reputation System) 是賽門鐵克領先業界防護功能的基石。檔案信譽資料庫維護超過 80 億個檔案的信任與惡意程度的評等。它每天處理超過 2,000 萬項新的信譽變更，讓每天有超過 400 萬個新檔案和簽章者新增至檔案信譽資料庫。維護所有檔案的即時信譽資料庫的優勢之一，就是可以快速偵測到進入到客戶網路的新惡意軟體，而不會有中斷業務運作的風險。

基於「信譽」惡意軟體偵測所面臨的挑戰，是某些用於識別惡意軟體的標記可能與賽門鐵克客戶開發和部署的自建應用程式的標記非常相似。這些標記可能包括以下項目：

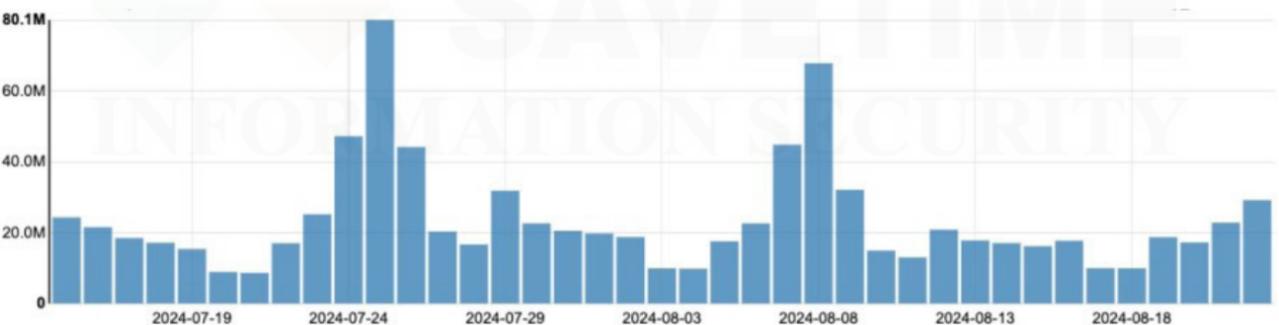
- 檔案在我們的使用者社群中並不普遍
- 檔案並非由可信賴的權威機構簽署
- 檔案會隨著新更新的推出而經常變更
- 檔案經常被混淆
- 檔案以多步驟安裝程式安裝，看起來像是多階段的惡意軟體攻擊

適用於各種情境是關鍵

為了成功攔截惡意軟體且不干擾業務運作，賽門鐵克檔案信譽系統會適應客戶的環境，並學習如何區分自行開發的應用程式與惡意軟體，即使許多跡象與上述相似。這些技術包括：

- 主動型白名單計畫 (Proactive Allow Listing Program)：可信賴的客戶可以註冊賽門鐵克主動允許清單程式，並提交自訂應用程式。
- 相似性分析 (Similarity Analysis) 以識別應用程式的更新：這包括根據相似度指標對檔案進行集結，並識別自行開發的應用程式的更新。
- 簽章信譽的可調適性 (Adaptive Signer Reputation)：賽門鐵克可辨識對您的組織而言是特定的簽章，並追蹤為「允許」的簽章者。
- 應用程式安裝標記：賽門鐵克使用啟發式方法來識別應用程式的安裝方式，這可能包括檔案安裝的位置、檔案與其他檔案的結合方式、檔案在您組織中時間、用於散佈檔案的 IP 位址等。

下圖顯示的是被過濾封鎖的自建應用程式「信譽」查詢數量。這個高效率的評級系統對於賽門鐵克的低誤報率 (FP) 貢獻良多。



欲深入瞭解「下載防護：下載鑑識」的詳細資訊，[請點擊此處](#)。

欲深入瞭解有關 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策，[請點擊此處](#)。



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更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, 把我們當成可信賴的資安建議者、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好用資源。

保安資訊連絡電話：0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>