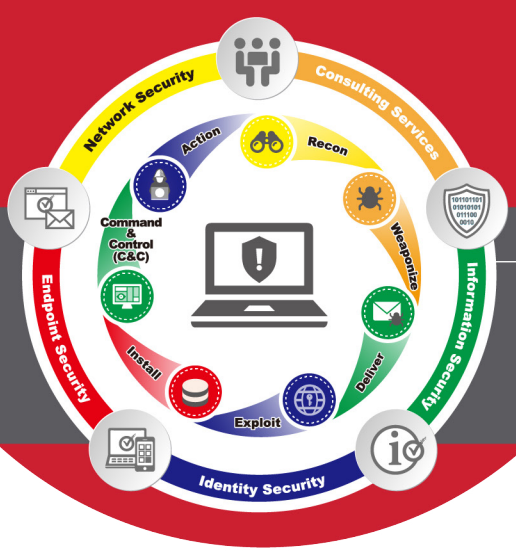


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克 IPS 引擎～新增 JA3 指紋識別技術智取迴避偵測手法的威脅

2025 年 5 月 20 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在現今快速演進的威脅環境中，網路罪犯不斷開發新技術以繞過傳統安全防護的偵測。以定義檔為基礎的偵測雖然仍有價值且需要，但惡意軟體作者可能會利用多樣態、變種和其他混淆方法來逃避偵測。在賽門鐵克，我們致力於透過不斷創新的安全技術來領先這些威脅。因此，我們很高興與您分享，我們先進的入侵防護系統 (IPS) 引擎現已結合 JA3 指紋技術，以提供更卓越的威脅偵測能力。

了解挑戰：真實世界中的迴避偵測手法的威脅

傳統的安全解決方案通常依賴識別已知的惡意程式碼模式或網路特徵。然而，現代惡意軟體的設計經常會改變其外觀和行為，使其很難僅使用這些方法來偵測。這些威脅可能會使用：

- 多樣態：改變程式碼結構以避免與特徵相符。
- 網域產生演算法 (DGA)：動態產生網域名稱以避開黑名單。
- 加密：加密通訊以隱藏惡意流量。

這些規避手法可讓惡意行為者在您的網路中建立據點，並在被偵測到之前造成重大損害。這就是 JA3 指紋技術發揮作用的地方。

JA3：更智慧的端點威脅偵測方法

JA3 是指分析 TLS／SSL(傳輸層安全／安全 Sockets 層) 用戶端和伺服器交握階段 (handshake) 特徵的指紋技術。這些交握是客戶端和伺服器建立安全連線時的初始協商過程。JA3 並非著重於加密通訊的內容，而是分析交握本身的具體細節，例如：

- 支援的 SSL／TLS 版本
- 提供的密碼套件
- 使用的 TLS 擴充套件

這些特性獨特組合為每個用戶端和伺服器建立獨特的指紋。惡意行為者經常在通訊中使用特定的函式庫或預先建立的工具，這會產生一致且可辨識的指紋，可利用這些指紋進行偵測。

JA3 如何增強賽門鐵克的 IPS 引擎

透過將 JA3 指紋識別功能整合至賽門鐵克的端點 IPS 引擎，賽門鐵克安全回應現在可以更有效地：

- 識別使用已知框架的惡意行為者：許多惡意軟體系列和攻擊套件持續使用特定的 TLS／SSL 配置。JA3 可讓 IPS 引擎識別這些模式，即使惡意軟體試圖混淆其程式碼。
- 偵測未知威脅：即使前所未見的特定的惡意軟體，只要它使用與惡意活動相關的 TLS／SSL 配置，IPS 引擎就能將其標示為可疑。
- 減少誤判及漏報：JA3 提供更精確的偵測方法，大幅提升警示的真實度。高精確度可減少誤報 (偽陽性、錯殺率)，同時消除流量偵測中的漏報 (偽陰性、漏網之魚)。

對您的組織的效益

使用 JA3 指紋技術強化賽門鐵克的端點威脅防護，可為您的組織帶來多項好處：

- 主動式防護：在執行前階段偵測並阻擋更多威脅。
- 改善安全態勢：針對複雜的攻擊加強端點防禦。
- 降低風險：將惡意軟體感染的影響降至最低。。

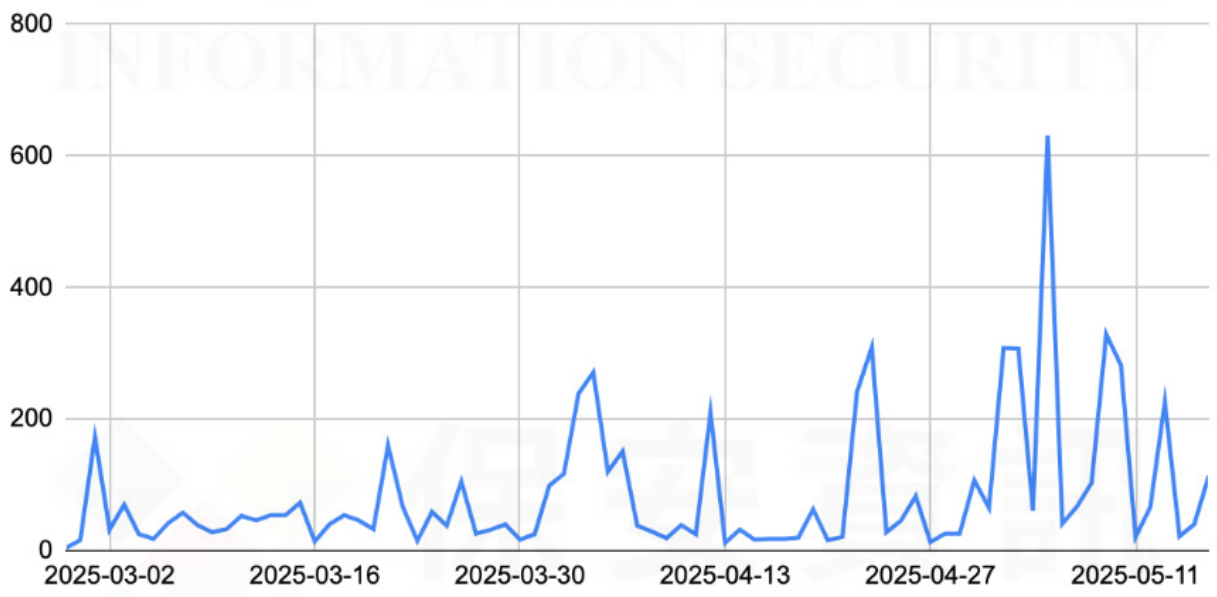
賽門鐵克優勢：由賽門鐵克安全機制應變中心 (Symantec Security Respons) 提供支援

值得注意，賽門鐵克防護技術的威力在於全球賽門鐵克安全機制應變中心團隊的監控與分析。IPS 引擎會根據指紋識別潛在威脅，而我們的專家則會根據最新的威脅情報持續監控和精進這些識別碼，確保端點受到最新威脅的保護。

可用於賽門鐵克雲端沙箱

JA3 指紋識別功能尚未在賽門鐵克產品中可直接設定或報告。不過，賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 提供此增強的威脅偵測功能。賽門鐵克雲端沙箱是一項後端服務，多項賽門鐵克產品利用這項服務來防禦前所未見新的、進階的、不斷演進的和目標性的攻擊。JA3 指紋偵測方法已證明可有效對抗 Dridex 惡意軟體和 Remcos 遠端存取特洛伊木馬等威脅。報告的偵測趨勢顯示，此功能可補足雲端沙箱的其他技術，增強其日常效能。

賽門鐵克雲端沙箱：基於 JA3 的 IPS 檢測事件



賽門鐵克堅定不移的承諾

在賽門鐵克 IPS 引擎中整合 JA3 指紋識別技術，代表我們在偵測和封鎖迴偵測手法威脅的能力上，向前邁進一大步。透過專注於 TLS／SSL 交握的基本特徵，我們可以識別惡意的行為者和模式，否則可能會被忽略。這項增強功能進一步鞏固賽門鐵克為客戶提供全面、主動安全解決方案的承諾。

建議客戶在桌機/筆電和伺服器上啟用 IPS，以獲得最佳保護。請點擊此處瞭解啟用 IPS 的說明。
讓網路威脅未攻先破--賽門鐵克的 IPS 入侵預防技術
欲瞭解如何整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站，請點擊此處。
沒有使用 SEP 也行？可使用賽門鐵克瀏覽器防護服務保護您的瀏覽器。

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**。