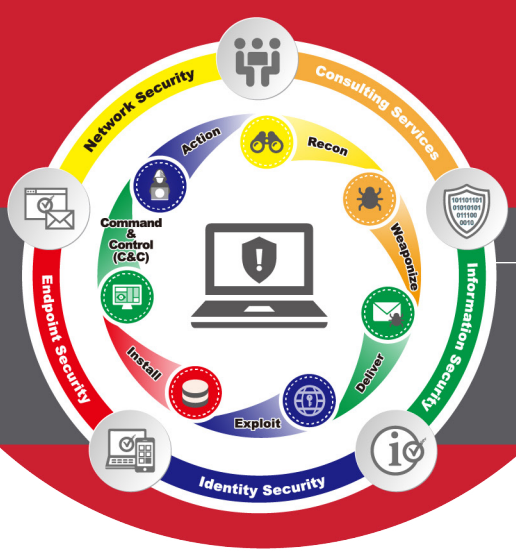


賽門鐵克雲端沙箱防護與洞察力

2025 年 5 月 13 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

面臨的挑戰

威脅份子不斷發展和精進其戰術、技巧和程序 (TTPs) 以利入侵目標並取得存取權限。這需要找出弱點，並從其他入侵成功的案例中學習，包括一些不常見的全新 TTPs，這些 TTPs 尚未受到完善的防護，或者以前所未見的掩護手法，突破現有防護機制的極限。

對抗惡意行為者的挑戰一直在於偵測、預防，甚至補救措施的成本和潛在風險與惡意軟體的開發和傳播相比，呈現出不對稱的戰爭。越來越多威脅所涉入的攻擊鏈中，日益濫用可信賴的工具和驅動程式，因此必須針對這些 TTPs 擬定詳細的訓練計劃以識別這些威脅、發現任何新技術，並揭露其內部結構，以便在這場戰役中取得優勢。

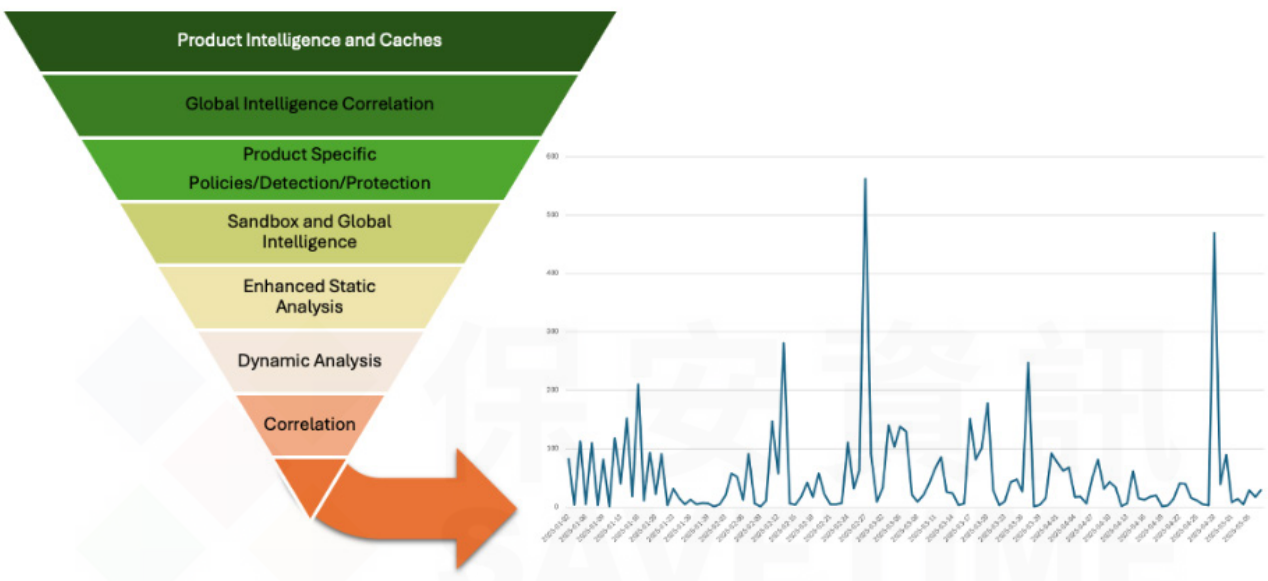
賽門鐵克雲端沙箱

賽門鐵克雲端沙箱能夠正面迎接挑戰，每天識別全新的威脅，為我們的客戶提供保護，並產生情報回饋至賽門鐵克全球情報資料庫，即使這些新技術正在威脅環境中散佈，也能有效瓦解它們。

賽門鐵克雲端沙箱不斷偵測到腳本類型的惡意軟體下載器、安裝程式和惡意竊密程式，當這些威脅使用新技術將惡意程式拆分到遠端有效酬載或隱藏在灰色地帶時，往往會造成偵測上的挑戰。GuLoader 和 MintsLoader 就是賽門鐵克雲端沙箱偵測到此類持續威脅的例子。由於賽門鐵克雲端沙箱採用多種引擎偵測技術會在威脅演變之前不斷發展，因此可持續保護系統。

在賽門鐵克雲端沙箱平台中，所有偵測與分析的引擎都被賦予充裕資源來進行游刃有餘之分析，此為不攔截的分析，得以讓惡意軟體盡可能展現其完整的面向，並讓沙箱內外的各種觀察家接收回饋，從惡意軟體與已知行為的落差以及威脅防禦措施的表現上獲取價值。賽門鐵克雲端沙箱中偵測數量的激增通常表示威脅份子正在引進新的技術或方法，這同時可讓所有賽門鐵克解決方案能共享威脅防護的量能。

電子郵件偵測在沙箱中的偵測技術達到高峰

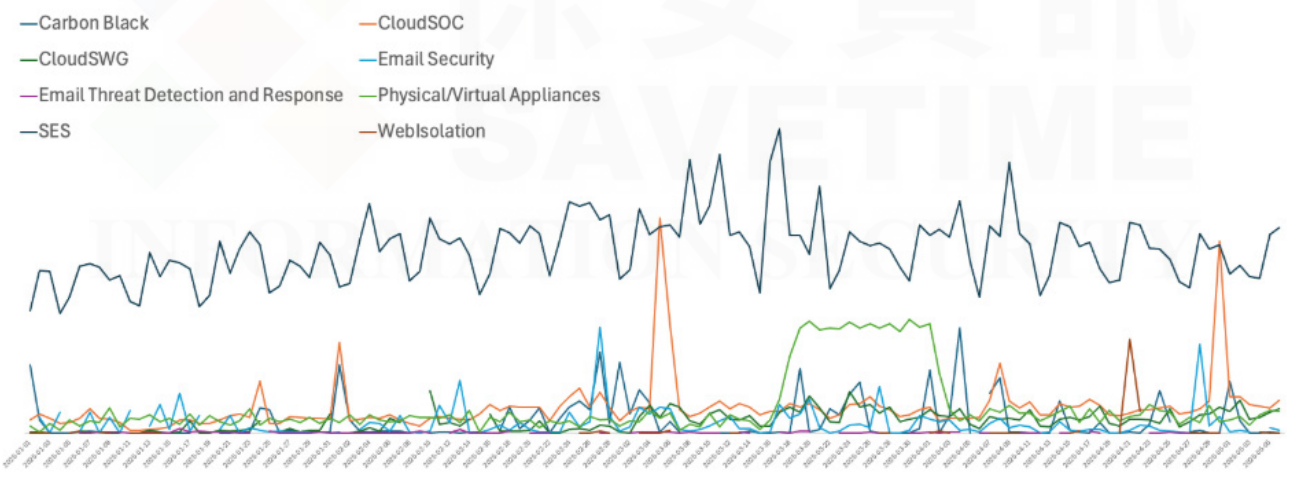


威脅情報--真正的寶藏

賽門鐵克雲端沙箱也可作為生成中介資料／詮釋資料 (metadata) 的來源，協助調查並提供有關威脅的強化資訊。某些賽門鐵克產品包含自動化功能，可將已知的惡意軟體和可疑樣本提交至賽門鐵克雲端沙箱，以蒐集額外的檔案相關資訊，SOC 或自動化系統可利用這些資訊進行威脅追蹤、分析或事件回應。賽門鐵克雲端沙箱透過與所有賽門鐵克產品的整合，提供跨網頁、電子郵件和端點等各種情境的威脅情報，並由多個內部工作流程加以運用，以強化威脅分析和回應程序，因此具有獨特的優勢。

下圖顯示賽門鐵克雲端沙箱提供給各個解決方案的偵測趨勢，因為產品的需求、涉及的威脅以及觀察到的可疑流量會隨著時間改變。

下列解決方案都會將惡意軟體提交至沙箱進行偵測／報告而讓彼此都能增強防護能力



被沙箱偵測為全新威脅的情報，將隨即提供給威脅回應團隊納入為已知的威脅資料庫，同樣威脅就不會再傳送到沙箱來重複偵測，這讓沙箱的處理能力永遠都保持餘裕，能以最快回應時間來偵測與回應前所未見的新威脅。

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端安全服務(Email Security.Cloud)的電子郵件掃描順序，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，請點擊此處。
欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的端點偵測和回應(EDR)功能，請點擊此處。

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**。