無形之牆：2025 年數十億次攻擊如何被阻擋

2026 年 3 月 4 日發布｜技術洞察

Parveen Vashishtha
(*帕爾文·瓦希什塔)
軟體研發總監
（威脅情報與研究）

賽門鐵克2025年遙測數據揭示當今威脅態勢的洞見

- **賽門鐵克的多層次安全防護體系於2025年攔截了約32億次攻擊，展現了現代企業級防禦縱深 (Defense in Depth) 的實際成效。**
- **IPS 承擔了主要防禦任務 (處理約 97% 的所有攔截工作)，它能有效減少後端安全營運中心(SOC)的負荷，讓團隊專注於處理剩下 3% 更隱蔽、更複雜的威脅 。這不僅大幅降低了受感染的風險，更重要的是透過「早期攔截」縮短潛伏時間，避免攻擊者有機會在內部網路進行橫向移動。**
- **數據揭示了當今網路安全領域中的壓力點集中在：網頁重新導向 (Web Redirection)、雲端規模惡意軟體與勒索軟體，這些威脅正被機器學習(ML)與行為偵測引擎(Behavior-based Engines)即時偵測並遏止。**

威脅情勢前所未見地嚴峻，但我們的深度防禦 (Defense in Depth)安全架構仍是現代防禦體系的穩固基石。2025年，賽門鐵克的安全技術在企業環境中攔截了約32億次攻擊。這組數據背後，是大規模的「層次化架構」(Layered Architecture) ——一道無形且堅不可摧的屏障，旨在及早阻斷威脅、縮短潛伏時間，並無論使用者身處何地皆能提供全面保護。

我們已準備好深入剖析去年各防護層的實際表現，並透過數據導向的分析佐證，揭示這些數據如何反映當今的攻擊手法轉變。

企業防禦的前線

入侵防禦系統 (IPS)

入侵防禦系統(IPS)持續作為賽門鐵克防禦體系的關鍵層級，負責阻擋幾乎所有重大攻擊。主要優勢包含以下幾點：

- IPS 攔截了～31 億次攻擊，佔所有被阻擋攻擊的 96.94%。
- 約95%的IPS封鎖措施皆在感染前階段執行，將組織面臨的風險降至最低。
- 這種感染前阻斷的主動防護機制至關重要，因其能在攻擊者建立立足點前攔截漏洞利用企圖的零時差虛擬補丁優勢——即使這些攻擊未攜帶惡意軟體酬載 (例如：透過伺服器漏洞竊取憑證的無檔案型攻擊)——進而為多層次防護的下一順位安全引擎 (例如：防毒軟體) 節省資源，並徹底消除感染風險。此項頂尖的端點防護能力使其有別於其他廠商的解決方案。

- 作業系統核心層級的入侵防禦系統(IPS)平均每日攔截690萬次攻擊，展現持續且大規模的威脅阻斷、抑制、中和的能力。
- 由作業系統核心層級的入侵防禦系統(IPS)攔截最多的是網頁伺服器漏洞，其阻擋次數超過9.64億次， 大大降低風險發生的機率或影響力。這項數據凸顯了網頁伺服器漏洞 (Web Server Vulnerabilities) 是當前網路安全的主要戰場。反映出攻擊者正高度自動化地利用已知漏洞進行大規模掃描與攻擊。

保護用戶邊緣

賽門鐵克網頁瀏覽器延伸功能

惡意網頁活動與惡意重新導向攻擊，仍是最常見的高風險攻擊途徑之一。賽門鐵克網頁瀏覽器延伸功能整合 Symantec 威脅情報到瀏覽器中，主動攔截惡意導向與網站。能在保護使用者免受惡意網站與重新導向攻擊侵害方面，扮演著關鍵角色。瀏覽器延伸是將功能和特性新增至 Web 瀏覽器的外掛程式。SEP 瀏覽器延伸會監控進出 Web 瀏覽器的 HTTP 和 HTTPS 流量，並在用戶端確定 URL 是惡意 URL 時攔截該流量。其防護實績如下：

- 賽門鐵克網頁瀏覽器延伸功能 攔截了5.453億次網路攻擊， 展現出卓越的防護覆蓋率。
- 其價值飆升，攔截數量較去年大幅增長～74.5%。
- 在攔截了3,500萬次惡意重新導向攻擊的同時，使用者得以免於接觸此最高阻擋類別中的高風險路徑。

利用雲端的彈性架構，確保檢測系統能維持高效能

雲端防護

雲端防護是一項關鍵的高流量防護層，在處理海量數據或應對瞬息萬變的威脅時，確保檢測系統能維持高效能。透過廣泛的威脅情報來防止攻擊，涵蓋多元的產品生態系統。以下是它抵禦威脅的實績：

- 攔截24億次威脅，抑制大規模的惡意企圖。
- 9.56億個攔截由機器學習引擎所貢獻，佔攔截威脅總數的最高比例。

已知威脅阻斷、抑制、中和的能力

靜態防護(防毒系統-AV)

靜態防護引擎層能阻斷、抑制、中和已知與新興威脅，強化入侵防禦系統(IPS)的預防能力，有效降低企業風險。以下是其去年展現的卓越防護功能：

- 靜態防護引擎 已阻斷、抑制、中和了7,250萬次威脅。
- 信譽引擎攔截了3,500萬次威脅。
- 機器學習引擎攔截了1,030萬次威脅。

雖然「預防性控制」 (例如：防火牆、入侵防禦系統 IPS) 能攔截大部分已知的威脅，但「靜態防護」扮演了關鍵的安全網角色。即使威脅穿透了第一線，靜態防護對於已知的惡意軟體家族而言，仍扮演著不可或缺的安全防護網角色。簡單來說：預防是為了減少接觸，而靜態防護則是為了確保「漏網之魚」無法在系統內執行。

行為防禦與零時差防護的實際運作

動態防護

我們的行為分析引擎專為捕捉靜態檢測方法所忽略的威脅而設計——特別是那些旨在規避靜態偵測的進階威脅與零時差攻擊。去年：

- 這些引擎成功攔截了超過 2600萬次威脅。
- 動態防護主動攔截了約98%的勒索軟體感染企圖——這對防禦零時差攻擊至關重要。

主動式伺服器與專業化防禦

我們的防護範圍亦涵蓋專業化與高價值環境，確保企業整體獲得一致的防禦能力。

- 企業伺服器防護：入侵防禦系統(IPS)共攔截2.882億次針對企業伺服器的攻擊。主要攔截威脅為網頁伺服器漏洞(1.178億次)與作業系統漏洞(4,290萬次)。
- Carbon Black(*碳黑)端點偵測與防禦：此功能針對常見勒索軟體家族，實現了約80%的主動阻擋覆蓋率。

企業整體安全防護

隨著賽門鐵克與Carbon Black(*碳黑)持續創新並擴展您的防禦體系，數據已充分證明成效。2025年，我們的防護能力成功阻擋數十億次攻擊，協助各類組織——即使是規模較小的團隊——維持強大的預防態勢。

穩健的現代化防禦體系需要具備深度、規模及跨多重防護層的無縫協調能力。這正是本架構所專為實現的目標——以不引起混亂 (安靜地)、維持高品質 (一致地) 且能支撐大規模業務 (企業級規模) 的情況下運行。

準備好將安全防護提升至最高等級？ 聯繫您當地的賽門鐵克與 Carbon Black 合作夥伴，瞭解這些企業級防護方案如何助您強化環境安全。

原廠網址：https://www.security.com/product-insights/billions-attacks-blocked-2025
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。2026/3

關於作者

Parveen Vashishtha(* 帕爾文・瓦希什塔)

軟體研發總監（威脅情報與研究）

Parveen 負責監督網路安全數據的彙整與傳遞，以及威脅導向的自動化偵測邏輯開發，負責帶領跨國團隊，涵蓋全棧防護 (Full Stack Protection)，包括入侵防禦 (Intrusion Prevention)、防毒軟體 (Antivirus)、端點偵測與回應 (EDR) 以及競爭情報 (Competitive Intel) 以強化主動威脅偵測能力。

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好用資源。

保安資訊連絡電話：**0800-381-500**。