賽門鐵克端點上的網路保護技術有何過人之處

2021年2月9日發布｜專家觀點

Kevin Haley
賽門鐵克安全響應中心總監

了解入侵保護系統 (IPS)

您可能不知道，我們端點防護／端點安全產品線中的入侵防護系統 (IPS) 技術有許多經長期實證的好效益。IPS 於 2003 年被加入我們的防毒軟體中，啟動我們端點防護產品第一次的重大技術創新。我們認為它非常重要，以至於我們更改了產品的名稱以反映 IPS 的導入。自 2003 年以來，我們曾因技術的更迭創新而多次更改產品的名稱，雖然在 2003 年可能是不正確的 (改名稱)。但是，我們在 IPS 方面是正確的。

10%

要真正了解 IPS，您需要從一個小的統計數字開始。IPS 可以辨識入侵網路對伺服器執行命令和控制 (C&C) 的惡意軟體。當惡意軟體試圖建立 C&C 通訊時，IPS可以阻止該流量並通知機器已被感染。這些功能僅是 IPS 所能做到的 10%，是 IPS 偵測的一小部分。還有其他 90% 重要的功能，用來保護端點，阻止來自網路的威脅。去年有 125 億次攻擊在感染前被 IPS 阻止。這些威脅在網路層就被阻止，因此它們甚至沒有進入機器。其中包括 31 億次針對伺服器的攻擊。所有這些機器都從未被攻破。因此也無需刪除或清除威脅。沒有警報被發送以佔用管理員 (Admin) 或安全運營中心 (SOC) 的時間。IPS 強大的預防措施能大幅降低偵測和回應 (EDR) 所需的的工作負荷。

90 億

IPS是專為防止「網路漏洞被開採利用」來發動攻擊而開發的專利技術。它尋找的是弱點特性與攻擊行為的特徵，而不是攻擊試圖傳遞的惡意軟體。它不在乎惡意軟體是什麼，攻擊行為甚至還達不到下載惡意軟體的階段就被阻止了。這是真正的主動式檢測和防禦。IPS 很完美的執行它當初被開發所賦予的任務。數字會說話，因為在 2020 年，它阻止了 90 億次這類攻擊。

>1

IPS的優異防護功能還不僅止於此。它還可以防止最多其他類型的攻擊。僅在2020年就攔截了以下幾種攻擊：

- 阻止 **30 億次** 網路攻擊，例如：表單劫持、惡意重定向和漏洞利用工具組。
- 阻止 **5.27 億次** 加密貨幣劫持和挖礦程式的攻擊。
- 阻止 **1.91 億個** 技術支援詐騙。

不僅如此……還有更多。IPS還可以識別經由網路以其他方式推送給您的惡意軟體。這些可能是上架在網站上的惡意軟體、試圖在您的瀏覽器中彈跳出的廣告軟體或正在下載的非必要的應用程式/可能有害的應用程式 (PUAs)。

- 阻止 **9.7 億個** 惡意軟體、廣告軟體和非必要的應用程式/可能有害的應用程式 (PUAs)。

70%

去年，賽門鐵克 IPS 總共阻止了近 140 億次攻擊，在保護端點的所有檢測中占了 70%。

IPS 是讓賽門鐵克與眾不同的關鍵技術之一。如果您是賽門鐵克端點防護 (SEP)、端點安全企業版 (SESE) 或端點安全完整版 (SESC) 的客戶，您就會有 IPS 來保護您。這些統計數字清楚地表明，這就是 IPS 為您所做的。

關於作者

Kevin Haley
賽門鐵克安全響應中心總監

Kevin Haley 負責確保來自賽門鐵克全球情報網路的安全內容，對其客戶而言是可操作的--包括關注安全問題的教育以及將安全內容整合到賽門鐵克的企業產品中。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/what-symantec-network-protection-endpoint-does-you
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。2021/2

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。