保安資訊--本周(台灣時間2025/01/17)賽門鐵克原廠防護公告重點說明

前言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 36 萬 8,600 台受保護端點上總共阻止了 4,260 萬次攻擊。這些攻擊中有 78.3% 在感染階段前就被有效阻止：**(2025/01/13)**

- 在**8萬400**台端點上，阻止了**1320**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬700**台端點上，阻止了**690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,400**台**Windows**伺服主機上，阻止了**5萬7,000**次攻擊。
- 在**5萬800**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬400**台端點上，阻止了**78萬5,400**次嘗試掃描在**CMS**漏洞。
- 在**4萬6,700**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**8萬7,900**台端點上，阻止了**170**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,600**台端點上，阻止了**99萬600**次加密貨幣挖礦攻擊。
- 在**10萬6,000**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**480**台端點上，阻止了**9萬7,200**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 17 萬 3,100 個受保護端點上阻止了總計 670 萬次攻擊。**(2025/01/13)**

- 使用網頁信譽情資，在 **166.3K** 個端點上阻止 **630** 萬次攻擊。
- 攔截 **17.3K** 個端點上 **275.7K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **7K** 個端點上攔截 **140.7K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **197** 個端點上攔截 **4.2K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2025/01/16

CVE-2024-55591--存在Fortinet FortiOS的授權繞過漏洞，已有漏洞攻擊嘗試實例

CVE-2024-55591 是最近發現的授權繞過漏洞，影響 Fortinet FortiOS 和 FortiProxy 產品。成功開採濫用此漏洞可讓遠端攻擊者透過精心製作的 Node.js websocket 模組請求，在有漏洞的裝置上取得超級管理員權限。此漏洞也隨著回報案例的增加，就在本週美國網路安全暨基礎設施安全局 (CISA) 已經其列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

賽門鐵克已經於第一時間提供多種有效保護(**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就內建的強化政策，將拒絕任何人建立管理帳戶或任何使用者群組。
- DCS 的 IPS 阻擋政策也會拒絕在防火牆設定中進行任何變更，而這些變更已在此漏洞攻擊中被觀察到。
- 此外，DCS 預設的 IPS 阻擋政策會停止所有入埠和離埠網路連線，以斷開脆弱系統與攻擊者的連線。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/01/15

CVE-2024-12686--存在BeyondTrust的漏洞已遭大肆開採濫用

CVE-2024-12686 是一個最近被揭露的作業系統指令注入漏洞，會影響 BeyondTrust 特權遠端存取 (PRA) 和遠端支援 (RS) 產品。如果被成功開採濫用此漏洞，現有管理權限的遠端攻擊者可能會在網站使用者的內容中注入任意指令。此漏洞已被在美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security 可針對 BeyondTrust 特權遠端存取應用程式的自訂沙箱與強化規則，可防止執行作業系統指令或上傳，以及利用此漏洞所報告的未經授權惡意程式碼的執行。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/01/14

防護亮點：IPS與WebPulse的聯防，形成超級團隊

賽門鐵克的入侵預防技術 (IPS) 可在威脅到達您的端點之前將其阻止。對於大型企業，賽門鐵克 IPS 負責 90% 以上端點防護與事件的可視性。

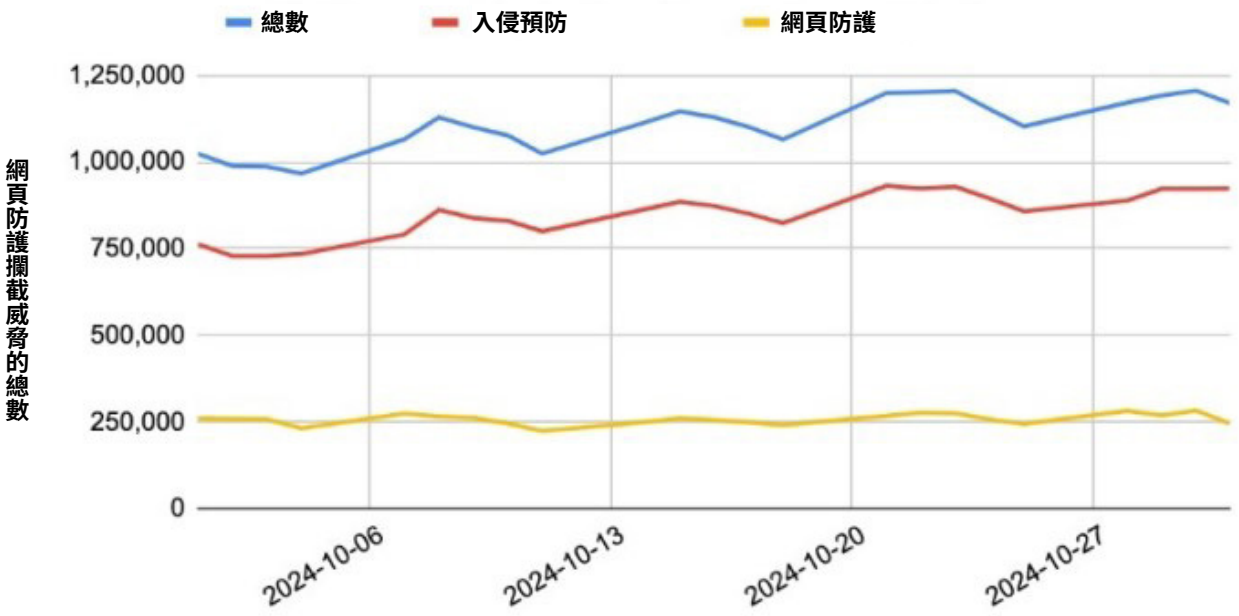
IPS 主要功能之一是網頁信譽 (URL Reputation)，利用的就是來自 WebPulse 網頁生態系的網頁、網域和 IP 位址分類服務來封鎖已知的釣魚網站和惡意軟體網域。網頁信譽功能增強入侵預防和瀏覽器防護功能。在入侵預防方面，會根據 WebPulse 檢查網路封包中觀察到的模式。對於瀏覽器防護，則根據 WebPulse 檢查網路瀏覽器的網路流量。

賽門鐵克的安全回應機制 (Symantec Security Response) 會持續監控威脅狀況，以辨識新的威脅、威脅物件和惡意網路活動。一旦發現新的威脅模式，WebPulse 服務會快速更新，以最大化保護所有整合此情資的賽門鐵克產品。例如：已知託管惡意軟體的網域會立即被歸類為惡意來源／惡意網路。了解有關 WebPulse 分類更多資訊，並檢視特定網頁的分類，請瀏覽 https://sitereview.symantec.com。

WebPulse 網頁生態系的網頁分類資料庫就像是隨時更新的動態封鎖清單。賽門鐵克端點代理程式以及其他賽門鐵克產品會詢問 WebPulse 有關網頁、網域和 IP 位址的資訊。WebPulse 提供的答案可用於即時偵測和防護決策。網頁信譽 (URL Reputation) 的強度也可以在 SEP 代理程式政策中調整。高強度偵測設定可針對「偵測層級」和「監控層級」進行調整。

賽門鐵克入侵預防和瀏覽器防護每天定期使用網頁信譽 (URL Reputation) 阻擋超過 100 萬個攻擊。以下是 2024 年 10 月攻擊遙測大數據的摘要大綱。

賽門鐵克 IPS 防護技術的高效攔截攻擊，有很大助力來自於 WebPulse 網頁生態系的情資



與 WebPulse 網頁信譽 (URL Reputation) 相關的 IPS 特徵 ID(客戶可在其偵測日誌中查閱)為：

- (入侵預防)29565 - Web Attack：Webpulse Bad Reputation Domain Request
- (瀏覽器防護)60501 - URL reputation：Browser navigation to known bad URL。

欲了解在桌上型電腦和伺服器上如何啟用入侵預防(IPS) 的詳細資訊，請點擊此處。
欲了解有關在 Windows 桌上型電腦上啟用 IPS 瀏覽器延伸防護，防止惡意網站的詳細資訊，請點擊此處。
沒有安裝 SEP？也能試用 Symantec Browser Protection 來保護瀏覽網頁的安全。
欲了解更多關於賽門鐵克雲端網頁安全引擎 (WebPulse)--網頁生態系的即時情資資訊，請點擊此處。

2025/01/14

Fireant進階持續威脅(APT)駭客組織最近進行中的惡意活動

Fireant (也稱為 RedDelta, Mustang Panda) 進階持續威脅 (APT) 駭客組織最近針對蒙古、台灣、緬甸、越南和柬埔寨散佈 PlugX 後門的最新變種。據報導，該組織最新攻擊還針對其他多個國家，使用惡意的 Windows 捷徑檔 (.LNK)、Windows Installer (MSI)、Microsoft Management Console (MSC) 和 HTML 檔案進行攻擊。為了逃避偵測，該駭客組織已知會利用 Cloudflare 內容傳送網路 (CDN) 來代理指令與控制 (C&C) 流量至攻擊者操作的伺服器。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/01/13

Ottercookie惡意竊密程式涉入國家級的駭客集團的加密貨幣竊取行動

OtterCookie 是一種專門用來竊取加密貨幣資訊的惡意竊密程式，最近觀察到被國家級的駭客集團使用。當使用者被誘騙下載偽裝成 NPM 或 Node.JS 專案的惡意程式載入器後，攻擊就會被觸發。一旦執行，惡意程式載入器會從遠端位置下載 JSON 資料，並繼續以 JavaScript 程式碼的方式執行 cookie 屬性。一旦被感染，Ottercookie 就能接收遠端指令和執行 shell 指令，並掃描被感染的機器，尋找包含加密貨幣錢包的文件或影像。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Cryxos!gen1
- Trojan.Gen.MBT

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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**。