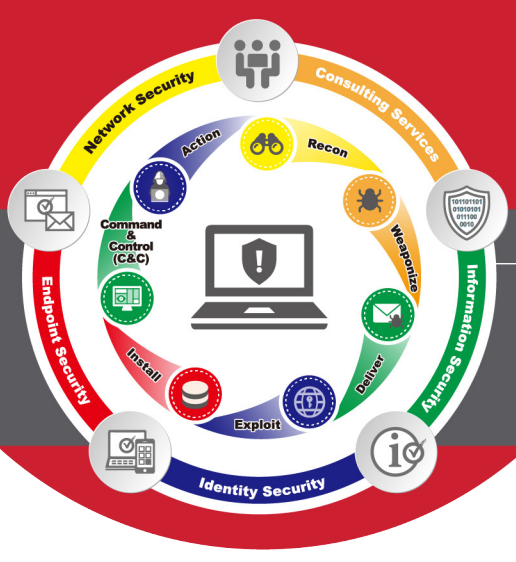


IPS稽核特徵改變遊戲規則的價值～有效攔截勒索軟體攻擊鏈中的RMM工具濫用

2025 年 7 月 1 日發布

在當今節奏快速的數位世界中，IT 團隊仰賴遠端監控與管理 (RMM) 工具來維持一切運作順暢。這些工具對於生產力來說是不可或缺的，但事實上，勒索軟體駭客組織正在利用這些工具入侵網路、部署惡意軟體，並脅迫 貴公司的業務。

但您如果能扭轉局面呢？如果您有一個預警系統，可以在可疑的 RMM 活動演變成昂貴的勒索軟體噩夢之前就發現它，那可以怎麼辦？

有了**賽門鐵克入侵防護系統 (IPS) 的稽核特徵功能**，您就可以做到。它們是您對付最陰險之勒索軟體攻擊的主動防禦工具。

詭異的威脅：勒索軟體如何劫持 IT 團隊仰賴遠端監控與管理 (RMM) 工具

勒索軟體駭客組織很聰，知道您使用合法的 RMM 工具，例如：AnyDesk、ScreenConnect、TeamViewer 和 Splashtop。他們不是以新奇的零時差入侵，而是濫用您賴以提高工作效率的這些常用工具軟體。我們已經看到頂尖的勒索軟體家族，例如：LockBit、BlackCat、Hive 和 AvosLocker 屢次濫用這些常見的 RMM 平台：

- 取得初始存取權
- 在網路中建立據點
- 在系統之間自由移動
- 竊取敏感資料
- 最後，釋放其破壞性的有效酬載

突破勒索軟體的挑戰：主動偵測、不中斷作業

這就是 IPS 稽核特徵創造巨大價值的地方。與其等待破壞發生，這些特徵會一直觀察，充當您的隱密守護者。

這就是核心價值主張：

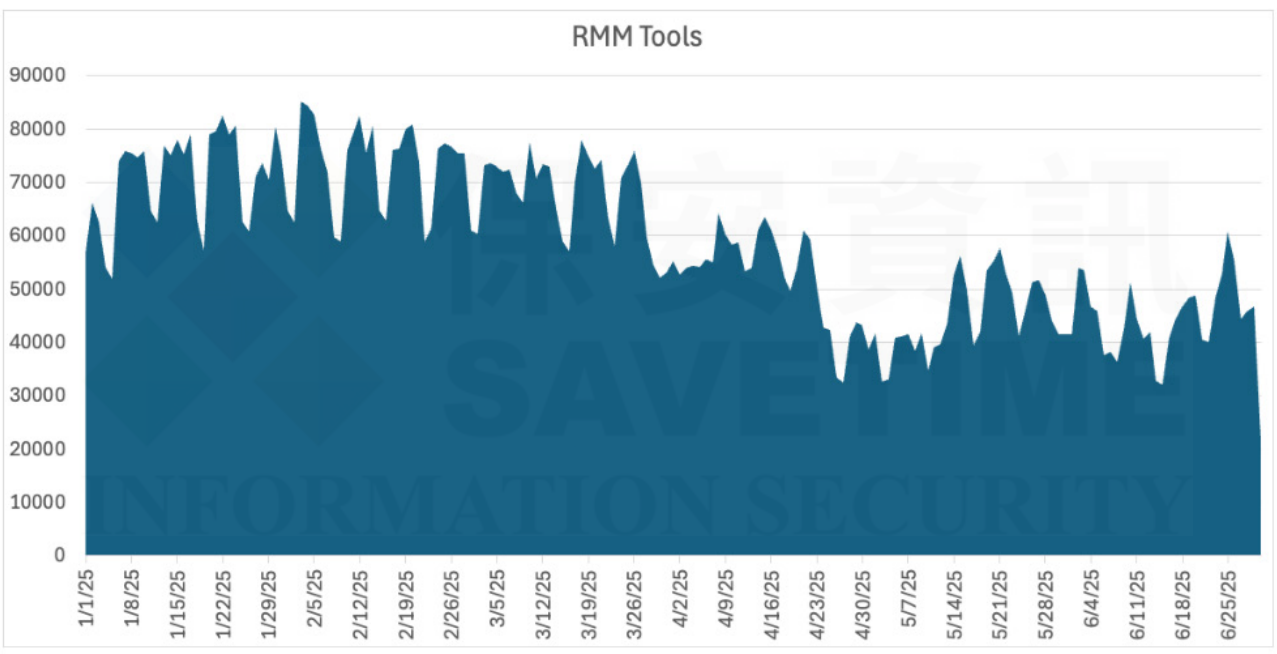
1. **早期預警，發揮最大的影響力**：IPS 稽核特徵會主動監控可疑的 RMM 行為：
   - 向外與 RMM 基礎架構的非預期連線
   - 未經授權的 RMM 代理安裝
   - 不尋常的遠端會話啟動和檔案傳輸。
2. **稽核模式**：預設情況下，IPS 稽核特徵以**稽核模式**運作，記錄所有活動並觸發警報。這可為您的安全團隊提供無價的早期可視性，讓您建立正常、經核准的 RMM 使用基準。這對於識別真正的威脅是非常重要的，而不會持續出現誤判。
3. **不會中斷 IT 的關鍵業務**：與可能會阻礙合法 IT 作業的解決方案不同，IPS 稽核特徵 (Audit Signatures) 專為精確而設計。您可以在不妨礙基本 IT 支援功能的情況下抓到壞人。建立基準後，您可以選擇性地將特定特徵切換至**封鎖模式**，主動防止風險最高的未授權或惡意 RMM 活動。
4. **強化您的資安監控中心 (SOC)**：對於您的 SOC 團隊而言，這些特徵可改變遊戲規則。它們可將模糊的懷疑轉換為可採取行動的情報：
   - **情境豐富的警示**：每個警示都提供重要的詳細資訊：哪個 RMM工具、來源／目的地 IP、時間戳記和活動類型。
   - **具體指出異常**：快速發現來自未經授權裝置的 AnyDesk 會話、可疑電子郵件後的 ScreenConnect 安裝程式，或非辦公時間的 ZohoAssist 使用情況。
   - **強化威脅攔截**：來自稽核特徵的豐富記錄可成為主動偵測威脅的寶貴資料，協助您揭露隱藏的攻擊者。
   - **統一安全態勢**：此遙測可與您的 SIEM 和 EDR 解決方案無縫整合，提供網路和端點活動的全面性整體檢視，以強化事件回應。

您的行動計畫：立即強化您的防禦

若要真正發揮 IPS 稽核特徵的威力，並大幅改善您的勒索軟體復原能力，請遵循此策略路線圖：

1. **大範圍的應用**：針對整個網路上所有已知的 RMM 工具啟用稽核特徵。
2. **針對您的環境調整**：針對您特定的網路使用情況微調這些特徵。這對於建立合法活動的精確基準、減少誤報並確保您的安全團隊專注於真正的威脅非常重要。
3. **優先進行每日檢閱**：優先進行每日警示檢閱，並將重點放在異常的端點、非工作時間的活動，或出現新的、未經核准的 RMM 工具。
4. **執行白名單**：維持經核准的 RMM 工具和授權管理員的嚴格白名單，以進一步簡化調查工作。
5. **策略性封鎖**：一旦確認正常行為，針對確定的威脅啟動封鎖模式，立即關閉惡意活動。

切換至封鎖模式後，賽門鐵克 IPS 稽核特徵會封鎖 RMM 工具



必須強調的事實：投資於主動式勒索軟體防禦

在對抗勒索軟體的戰鬥中，早期偵測不僅是一項優勢，更是一項必要條件。透過部署稽核模式 IPS 特徵碼，您可以為組織提供主動、不中斷且高效的方式，偵測濫用 RMM 工具以來 發動勒索軟體攻擊的關鍵階段。這項功能對於預防會造成後患無窮的入侵、保護您的資料，以及確保持續的業務運作至關重要。

儘早做好萬全準備，不要坐等勒索軟體來襲。使用賽門鐵克稽核模式 IPS 特徵碼 (Symantec IPS Audit Signatures) 能加強您的防禦能力，翻轉網路威脅的趨勢。

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。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**。