Symantec
A Division of Broadcom

產品型錄

Symantec Endpoint Detection and Response

迅速的威脅搜尋及矯正方式

快速一覽

偵測與揭露 – 縮短發現洩漏的時間並迅速揭露入侵範圍

- 採用機器學習和行為分析來揭露可疑活動、偵測資安事端並排列優先順序
- 為可疑程序檔及記憶體刺探利用自動辨識並產生資安事端
- 運用程序記憶體分析來揭露針對記憶體的攻擊

調查與遏止 – 提高資安事端回應者的工作效率，確保威脅抑制

- 透過持續性記錄端點活動來確保完整記錄資安事端，檢視特定端點的流程
- 即時搜尋所有端點的入侵跡象，尋找威脅
- 以端點隔離的方式在調查期間封鎖可能遭到入侵的端點

解決 – 迅速修正端點，確保威脅不會再次入侵

- 刪除受影響端點上的惡意檔案和相關跡象
- 將端點上的檔案加入黑名單和許可清單
- 增強的報告功能可匯出表格作為資安事端解決報告

整合及自動化 – 統合調查人員觀點、協調資料及工作流程

- 輕鬆整合資安事端資料及行動至現有 SOC 基礎架構，包括 Splunk 及 ServiceNow
- 運用自動化資安事端教戰守則中的規則，來複製技術純熟的調查人員採用的最佳實務準則和分析
- 運用自動化跡象收集，取得端點活動的深入能見度

企業正逐漸處於複雜攻擊的威脅陰影之下。事實上，研究已發現威脅潛藏在客戶環境中的平均天數為 190 天[1]。這類進階持續性威脅會利用各種隱藏技術來閃避偵測，繞過傳統安全防線。一旦進階攻擊取得進入客戶環境的管道，攻擊者便能使用許多工具來閃避偵測，並開始刺探利用珍貴的資源和資料。資安團隊在試圖偵測和完整揭露進階攻擊的影響範圍時，會遭遇到許多難題，例如需要人工搜尋分散孤立的大型資料來源、缺乏對於重要控制點的能見度、誤報導致警示疲乏、難以辨識和修復受影響端點。

Symantec EDR 解決方案

Symantec EDR 透過精準的機器學習及全球威脅情報揭露進階攻擊，盡可能減少誤報，協助確保安全團隊的高生產力。Symantec EDR 功能讓資安事端回應者快速搜尋、辨識和控制所有受影響的端點，同時使用各種內部部署沙箱和雲端沙箱來調查威脅。Symantec EDR 也利用自動化調查教戰守則及使用者行為分析，提高調查人員的生產力，並將最有經驗安全分析師所握有的技能和最佳實務準則帶給任何企業組織，進而大幅降低成本。

[1]「Ponemon 的 2018 年資料外洩成本報告」https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmld=55017055USEN&

此外，持續及隨選的系統活動記錄，則支援完整的端點能見度。Symantec EDR 在端點利用進階攻擊偵測，並以雲端型分析偵測目標式攻擊，例如入侵偵測、指令和控制信號、橫向移動，以及可疑的 PowerShell 執行。

提高調查人員工作效率

Symantec EDR 可根據風險等級排定資安事端的優先順序，藉以提高調查人員的工作效率。Symantec EDR 還會針對賽門鐵克目標式攻擊分析 (Target Attack Analytics) 及動態攻擊者情報 (Dynamic Adversary Intelligence) 辨識的目標式攻擊，自動產生資安事端。

此外，調查人員也可以利用端點活動記錄功能來追蹤攻擊跡象並執行端點分析。Symantec EDR 支援各種事件的連續及隨選擷取，包括階段作業、流程、模組載入點修改、檔案與資料夾操作、登錄變更及網路連線活動等。

根據賽門鐵克網路安全威脅研究報告 (ISTR) 所述，超過 20% 的惡意軟體具有虛擬機器感知能力，也就是可躲開傳統沙箱的偵測功能。Symantec EDR 採用多種進階技術 (包括模仿人類行為)，可偵測出此種能夠感知虛擬機器的威脅，如有必要可使用實體伺服器加以觸發。

Symantec EDR 提供智慧型資安事端警示，可提高調查人員的工作效率

雲端型攻擊分析及端點進階攻擊偵測

Symantec EDR 包含目標式攻擊分析 (TAA)。TAA 可分析全球各種好壞活動，涵蓋構成遙測組合的所有企業。我們的雲端型人工智慧演算法及進階機器學習，可自動依據新的攻擊技術做出調整。TAA 會產生即時資安事端，詳細分析攻擊者、技術、受影響機器及矯正方式指導，並將其串流至 EDR 主控台。這種方式可簡化資安事端回應者的工作，並協助整體安全團隊提升生產力 (使用 Advanced Threat Protection 3.1 以上版本的賽門鐵克客戶，可免費獲得 TAA)。

Symantec EDR 也利用端點行為政策，由賽門鐵克研究人員持續更新，以便在端點立即偵測進階攻擊方法 (目前有 330 種以上)。這些偵測會詳述可能顯示攻擊進行中的活動，包括檔案及登錄變更、可疑的網路及程序活動，以及使用可在現有程序啟動惡意執行緒的特定 Windows API。

追蹤端點間的異常情況

Symantec EDR 提供軟體、記憶體、使用者和網路基本活動的全面性檢視，進而簡化環境內的攻擊者搜尋。攻擊者在環境中有所行動時，他們的惡意軟體和使用者活動便顯示為異常。

Symantec EDR 會偵測這些環境中的不速之客，包括：

- **軟體異常** – 揭露安裝罕見軟體、組建不一致、搭載老舊或未修補作業系統 (OS) 版本的端點
- **記憶體異常** – 運用程序記憶體、檔案和 OS 物件及系統設定的鑑識調查，偵測記憶體內的不速之客
- **使用者異常** – 使用者行為分析，能偵測偽裝成合法使用者卻執行異常活動的攻擊者
- **網路異常** – 運用數據分析來辨識異常 IP 位址，另一方面運用信譽查詢來辨識與資料洩漏相關的 IP 位址和網域

這些異常偵測會透過雲端型服務提供，並可使用內建教戰守則，針對各種異常活動產生特定報告。

MITRE ATT&CK 事件擴充及網路分析

Symantec EDR 提供各種工具，依據 MITRE ATT&CK 架構偵測及視覺化攻擊生命週期。EDR 工具會依據 ATT&CK 矩陣中的戰術與技術，說明各種攻擊方法。此外，快速篩選功能可讓調查人員輕鬆將結果範圍縮小至 MITRE ATT&CK 生命週期的一或多個階段，包括初始存取、持續存在、橫向移動及指令和控制。

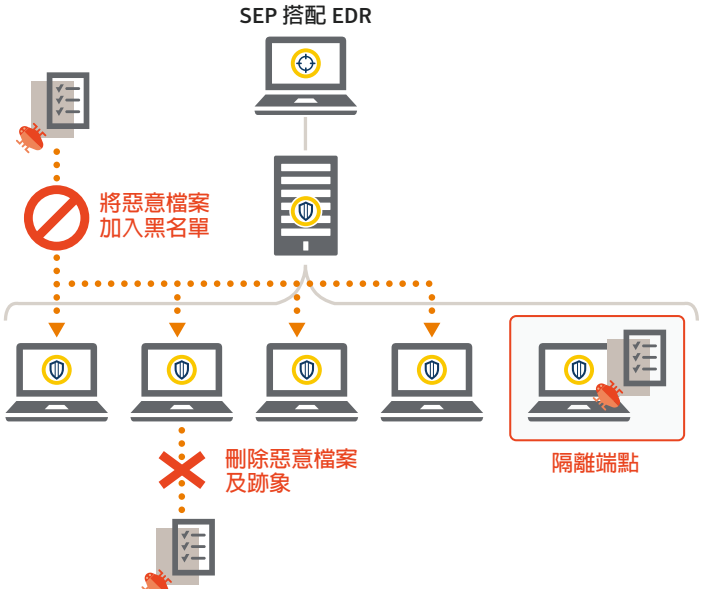
其中的關鍵在於 Symantec EDR 可透過自動化調查教戰守則支援 MITRE 網路分析。MITRE 建議企業實作零信任方法，透過以下方式進行鑑識收集與調查：詢問自動執行差異、可疑執行位置、可能的 DDL 注入及 SMB 事件監控。Symantec EDR 可在端點之間輕鬆執行排程掃描，以判定是否能利用 MITRE 攻擊者模式社群的一般知識偵測任何攻擊。

完整迅速的端點修復

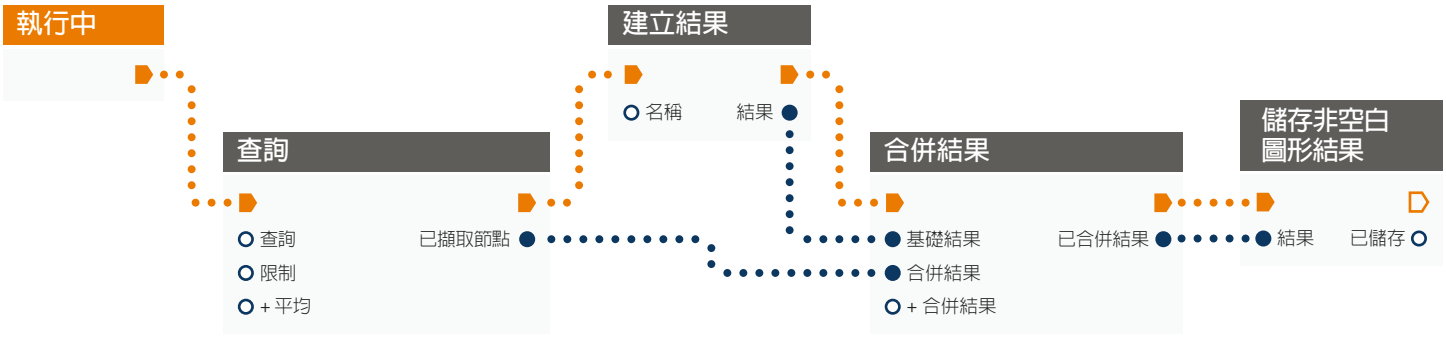
Symantec EDR 可迅速修復受影響的端點，包括檔案刪除、加入黑名單及端點隔離。使用 Symantec Endpoint Protection (SEP) 內建的強大清除功能，回應者可由單一主控台採取行動，只要按一下便能在多個端點套用修正方法。

自動化技術純熟調查人員的實務做法

Symantec EDR 支援教戰守則，能夠自動化安全分析師的複雜多步驟調查工作流程。內建教戰守則，可快速揭露可疑行為、未知威脅、橫向移動和政策違規。安全團隊可以檢視教戰守則來學習專家級搜尋和調查技術。此外，調查人員可以建立自己的教戰守則，以便自動化最佳實務準則，並記錄特定的威脅搜尋情境。



Symantec EDR 可確保端點回到感染前狀態



Symantec EDR 具有強大的自動化教戰守則，可進行跡象收集、調查及回應

彈性的部署選項

Symantec EDR 是彈性的解決方案，可在內部部署或雲端部署。Symantec Endpoint Protection (SEP) 客戶可利用 SEP 單一代理程式架構中整合的 EDR 功能。企業利用內部部署的 EDR 設備，就能迅速將 EDR 部署至現有 SEP 環境。此外，客戶可新增模組提供能見度，並與網路及電子郵件事件建立關聯 (電子郵件模組需要 Symantec Email Security.cloud)。

安裝或未安裝 SEP 的端點，都可利用可分解用戶端及內部部署收集伺服器 (或選用的收集服務代理程式)，在雲端型入口網站進行網路資料分析、鑑識分析及調查自動化。Symantec 雲端型 EDR 功能只要幾分鐘就能部署完成，迅速由端點收集資料，不會影響一般使用者體驗。

擴充您的 SOC 團隊

Symantec Managed Endpoint Detection and Response 是全年無休的鑑識調查及威脅搜尋服務，其中採用賽門鐵克 SOC 分析功能，主動偵測秘密攻擊，並以專業技術檢驗可疑活動。這類分析使用 Symantec Endpoint Detection and Response (EDR) 搭配機器學習分析，並與賽門鐵克全球威脅情報網路 (GIN) 建立關聯。

此外，Symantec EDR 客戶可由賽門鐵克 GIAC 認證的 SOC 分析師獲得資安事端分類及指導，無需負擔額外費用 (由 EDR 主控台以「接觸資安事端回應者」名義提供)。

賽門鐵克 Managed EDR 提供無可比擬的專業技術及全球規模，以下列功能支援安全團隊：

- 指派給每位客戶 GIAC 認證的賽門鐵克 SOC 分析師
- 採用 Symantec Endpoint Detection and Response 技術
- 內部部署及雲端的鑑識調查
- 針對新興的 IoC、TTP 及 MITRE ATT&CK 戰術，進行主動及受管理的威脅搜尋
- 預先授權遏止遭到入侵的端點
- 巨量資料分析及賽門鐵克全球威脅情報網路 (GIN) 關聯性
- 迅速免費的引導，以及持續的客戶參與

Managed EDR 結合 Symantec EDR 工具，新增許多 SOC 團隊需要的額外專業及全球涵蓋範圍。

強化安全投資

賽門鐵克的整合式網路防禦方法，可強化企業在安全基礎架構的現有投資。Symantec EDR 解決方案與安全性作業工具整合，提供事件與資安事端管理、問題單、自動化及協調功能，其中包括：

- 預建應用程式，適用於 Splunk、IBM QRadar 及 ServiceNow
- 整合式自動化及協調，使用 Phantom、Demisto 及 CyberSponse
- 開放式 API 涵蓋偵測、調查及回應功能

要求

如需 Symantec EDR 的完整要求，請造訪我們的系統要求頁面：

https://www.symantec.com/products/endpoint-detection-and-response#requirements

若要進一步瞭解 Symantec EDR 及 Symantec Managed EDR，請造訪我們的產品頁面：

https://go.symantec.com/edr

https://go.symantec.com/managed-edr

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw

19C199684_ds_EDR_TW