# McAfee Enterprise Log Search

**高速搜尋數十億個事件，更快速地找出問題所在**

資安團隊需要工具，以在警示與日俱增的環境中更快速地移動。這些團隊的分析人員需要存取更豐富的內容，並能快速查明與事件相關的詳細資料。McAfee® Enterprise Log Search 透過超快速搜尋原生未壓縮事件資料，來加速威脅搜尋作業。Elasticsearch 為後端提供技術支援，可最佳化查詢效能，讓您即時存取原始記錄。增強的搜尋功能，以自然語言輸入簡單關鍵字和更為精密的規則運算式模式均可進行查詢，進行目標式資料擷取作業。

## 主要優勢

- 最佳化記錄管理功能，適用於保留記錄保留和進行快速搜尋
- Elasticsearch 為後端提供技術支援，可達到高速擷取、編列索引和查詢效能
- 自然語言搜尋
- 可以輕鬆快速地將剖析資料檢視轉換為原始記錄
- 可與 McAfee Enterprise Security Manager 完全整合
- 靈活的部署選項，包括實體和虛擬裝置 (立即可供混搭使用)

## 最佳化記錄管理

McAfee Enterprise Log Search 是以 Elasticsearch 為基礎所建立，Elasticsearch 是一種利用反向索引以儲存資料的技術。結構中的反向索引目錄資料有助於有效擷取搜尋字詞。Elasticsearch 專為高效能擷取和編列索引所設計，McAfee Enterprise Log Search 因此可在擷取和編目後，高速搜尋原始資料。

McAfee Enterprise Log Search 是 McAfee® Enterprise Security Manager 的元件，為安全性資訊和事件管理 (SIEM) 解決方案。另一個輔助元件是 McAfee® Enterprise Log Manager，其設計目的是根據雜湊 (MD5) 入埠原始記錄來儲存記錄，藉此以獲取鑑識完整性，並壓縮這些原始記錄，以提高儲存效率。結合使用時，這兩個元件提供可同時使用的專用儲存解決方案，充分發揮快速搜尋 (透過 McAfee Enterprise Log Search) 與保留記錄以遵循合規性 (透過 McAfee Enterprise Log Manager) 的優勢，讓客戶不必妥協於只能二選一，可盡享受完整功能。

有了 McAfee Enterprise Log Search，您可以自訂保留原則，以在不同的年度期間 (365 天)、季度 (90 天) 或月 (30 天) 內儲存未壓縮的資料。使用者可以識別要與 McAfee Enterprise Log Search 建立關聯的資料來源，並新增最多六個單獨的保留原則。

## 與我們聯絡

## 增強式搜尋功能

McAfee Enterprise Log Search 中的搜尋功能類似常用的搜尋引擎，可進行自然語言輸入。可以從簡單的文字或關鍵字擷取搜尋結果。此外，也可以使用更複雜的模式，包含布林邏輯、萬用字元和規則運算式 (RegEx) 進行搜尋。若要進一步縮小搜尋結果範圍，使用者可依資料來源和日期套用篩選條件。日期篩選可讓使用者從產生記錄事件的時段中選擇，例如，最後一小時、當天、前一年，或自訂範圍。

## 與 McAfee Enterprise Security Manager 整合

與 McAfee Enterprise Security Manager 緊密整合，分析人員只需按一下，即可從剖析資料轉移到原始資料。在 McAfee Enterprise Security Manager 中產生事件時，已剖析的事件檔案將直接連結到來源記錄檔案和特定原始記錄。對於想進一步掌握該記錄或其中一部分的分析人員，可以僅選取有問題的記錄，以提示原始記錄搜尋。無需採取額外步驟，也不必啟動應用程式或介面，即可使用原始記錄搜尋進行更深入的偵測。

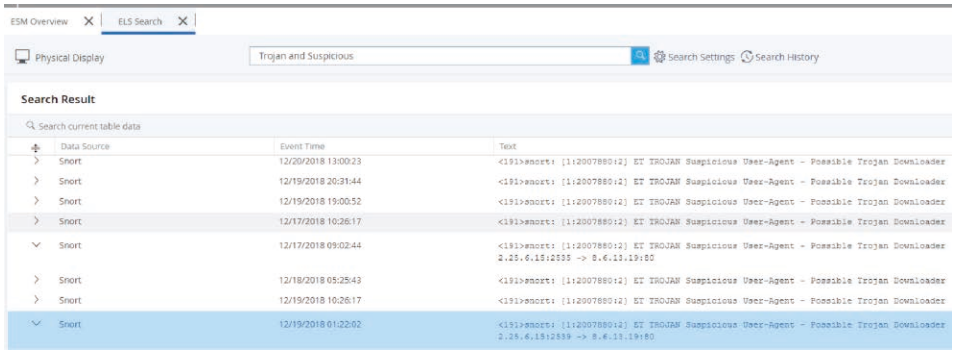


圖 1. 使用布林邏輯搜尋關鍵字，以揭露包含特洛伊木馬程式的可疑事件。

## 彈性部署與價格

彈性的傳送選項，包含實體裝置與虛擬裝置。依據內嵌特定每秒事件數量 (EPS) 的能力，而非每個資料來源的價格、每 EPS 的價格，或依照已編列索引之資料磁碟區的價格，來評估和銷售設備。虛擬機器 (VM) 以相同的原理獲得授權，並根據支援特定 EPS 所需的 CPU 核心數目進行銷售。這讓客戶可視需要新增額外的核心，而無需更換硬體。

## 收集並快速搜尋所需資料

部署 McAfee Enterprise Log Search 時，通常會使用六種類型的記錄來搜尋威脅。這些記錄可針對安全性事件提供特定見解與內容。

| 記錄類型 | 常用資料 |
| --- | --- |
| DNS 記錄 | ▪ 查詢的網域名稱<br>▪ DNS 查詢的來源 IP 位址<br>▪ DNS 查詢的成功或失敗<br>▪ 如果查詢成功，則會解析 IP 位址<br>▪ 回應的 TTL 值<br>▪ 使用的 DNS 伺服器 |
| Proxy 記錄 | ▪ 要連線的網域/IP 位址<br>▪ 已傳輸的位元組<br>▪ 連線的時間戳記<br>▪ 要使用的 URI<br>▪ 參照<br>▪ 使用者代理程式字串 |
| SMTP 記錄 | ▪ 電子郵件寄件者網域<br>▪ 電子郵件主旨<br>▪ 寄件者 IP 位址 |
| Windows 記錄 | ▪ Windows 安全性記錄事件<br>▪ Windows 應用程式記錄事件<br>▪ Windows 系統記錄事件<br>▪ Windows 程式碼完整性記錄事件 |
| DHCP 記錄 | ▪ 來源 MAC 位址<br>▪ 授與的 IP 位址<br>▪ 租用期間<br>▪ 要求與租用授權的時間戳記 |
| VPN 記錄 | ▪ 來源 IP 位址<br>▪ 驗證身分<br>▪ VPN 連線建立的時間戳記<br>▪ 連線類型：繼續執行或全新<br>▪ 驗證嘗試失敗 (若有) 以及對應的身分 |

## 深入瞭解

如需相關資訊，請造訪 **https://www.mcafee.com/enterprise/zh-tw/products/siem-products.html**

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw