McAfee Enterprise Log Manager

透過自動化的記錄收集、儲存及管理，降低遵循法規所需的成本。

透過正確地收集並儲存記錄，因為對不可否認的活動有了明確的稽核追溯，將可降低符合性的成本。McAfee® Enterprise Log Manager 可有效收集、壓縮及儲存所有的記錄檔。與 McAfee Enterprise Security Manager 整合後，可提供進階的搜尋、分析、關聯、警示與報告功能。所有事件和警示都可讓您既輕鬆且一鍵存取原始的來源日誌記錄，因此您的鑑識工作將可變得更有效率。

主要優點

- 通用的記錄收集與存留，可因應符合性需求
- 具有彈性的儲存與存留功能，適用於各種記錄來源
- 支援監管鏈與鑑識
- 記錄分析與搜尋
- 可將記錄儲存於本機，或透過受管理的儲存區域網路加以儲存
- 可與 McAfee® Enterprise Security Manager 完全整合
- 彈性的混合式傳送選項，包含實體裝置與虛擬裝置

對於記錄檔，McAfee Enterprise Log Manager 會加以收集、簽署並儲存。McAfee 可將所有記錄類型的記錄管理與分析工作自動化，包括 Microsoft Windows 事件記錄、資料庫記錄、應用程式記錄與 syslog。記錄會受到簽署與驗證，以確保其真實性與完整性 - 這是符合性的要件。現成可用的符合性規則集與報告，可讓您更輕易地證明組織遵循法規並強制原則的狀態。

使用此一密切整合的記錄收集、管理與分析環境不僅可強化您的安全設定檔，也可大幅提升您遵循 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA 與 SOX 等標準的能力。

智慧型記錄管理

McAfee Enterprise Log Manager 會進行智慧型的記錄收集，除了會針對符合性儲存適當的記錄外，也會針對安全性剖析及分析適當的記錄。您可以視需要保留原始格式的記錄，沒有時間限制，以支援您特定的符合性需求。我們不會變更原始記錄檔，因此 McAfee 支援監管鏈與不可否認性證明工作。

資訊存留需求不盡相同，除了取決於記錄來源外，也會隨著您的符合性需求而不同。McAfee Enterprise Log Manager 使用容易自訂的儲存集區，以確保您能夠正確儲存適當時間量的記錄。您可選擇最符合您需求的儲存選項，例如裝置上的硬碟儲存空間，或是可用於高速儲存區域網路 (SAN) 的選購光纖網卡。

我們無法單憑記錄檔獲知一切所需資訊。這些檔案包含了重要的證據，也是建立監管鏈很關鍵的一環，但它們同時也衍生出嚴重的安全問題。例如，我們在存取記錄中可能會看見某個使用者名稱，但卻找不到該使用者的角色或權限的相關資訊。我們也可能知悉所存取的系統為何，但卻對該系統所使用的資訊類型或擁有該系統存取權的使用者一無所悉。

與 McAfee Enterprise Security Manager 整合

McAfee Enterprise Log Manager 是 McAfee Enterprise Security Manager 中可選購的整合式元件之一。McAfee Enterprise Log Manager 能夠儲存記錄，而 McAfee Enterprise Security Manager 則可進一步深入剖析、標準化及分析記錄資訊，使其立即可供即時安全性調查與事件回應使用。

安全性事件產生時，剖析的事件檔案將會直接連結至來源記錄檔，以及特定的日誌記錄，讓您在事件管理與鑑識程序期間可以一鍵存取。您無須手動執行其他步驟、啟動其他應用程式，或費時搜尋記錄。

有豐富的內容可用於分析

McAfee Enterprise Security Manager 與 McAfee Enterprise Log Manager 的結合將可提供每個記錄的相關內容，使得每筆剖析的日誌記錄更具價值。其中可包含下列資訊：

- 來源或目的地 IP 位址
- 身分識別內容
- 所使用的主機名稱或服務
- 來自弱點評估掃描程式的弱點資訊
- 網路拓撲資訊
- 原則與隱私權資訊

彈性的儲存集區

McAfee Enterprise Log Manager 儲存集區在長期存留記錄的方式上增添了彈性。儲存集區是可用儲存裝置的虛擬群組，可在實體儲存裝置 (本機儲存裝置、NFS、SAN、CIF 等) 的各個群組間進行分配，以因應不同的記錄管理需求。

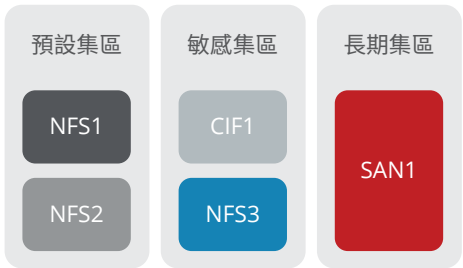

圖 1. 彈性的儲存集區可支援自訂記錄存留。

一個儲存集區可包含多個裝置，而資料可根據來源裝置指派至特定的集區，因此記錄能夠根據其與安全性、符合性、機密性或其他準則的關聯，儲存在個別的位置中。例如，對於符合性極為關鍵的記錄，可儲存在包含多個備援網路儲存裝置的集區中。較不關鍵的記錄，則可儲存在備援性較低的系統上；而對於鑑識用處最大的記錄則可儲存於本機上，以便快速進行分析。

快速部署

McAfee Enterprise Log Manager 與 McAfee Enterprise Security Manager 可透過單一合併裝置共同部署，或是分別進行配置，如此，即便是最大型的企業網路也可支援。彈性的混合式傳送選項，包含實體裝置與虛擬裝置。

與您的基礎架構整合

大部分的記錄管理解決方案多半是獨立運作的，但 McAfee Enterprise Log Manager 卻能夠與其他資訊安全系統協調運作。它可透過 McAfee Enterprise Security Manager 連線至您其他的安全基礎架構，以簡化安全性作業、改善整體效率並降低成本。因此，智慧型記錄管理將可與分析、網路檢查、資料庫事件監視等強大功能整合在一起。

深入瞭解

如需相關資訊，請造訪 **www.mcafee.com/tw/products/siem/index.aspx**。

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