McAfee Active Response

全方位的端點偵測與回應

注重安全性的組織現今正面臨一個急遽變化的威脅環境。攻擊方式日新月異、層出不窮，傳播速度也快得令人措手不及。「量身打造」的攻擊會利用目標明確的資訊來提升攻擊效力、降低被偵測到的可能性，以鎖定個別的組織。攻擊者突破防禦技術的案例日漸增加，目光長遠的組織亟需易於使用的整合工具，來協助組織進一步偵測出攻擊者的存在，以便快速進行調查及修補。最好的偵測與回應解決方案即使從日益增加的系統取得越來越多資訊，提供的安全效率也能有增無減。McAfee® Active Response 提供優異的預設功能、與現有安全性管理解決方案自動整合，以及使用者自訂，可大幅降低攻擊者傷害您的運算資產與公司品牌的機會。

主要優點

- **自動化：**擷取並監控內容和系統狀態，檢查是否存在可能是攻擊指標的變化，以及找出潛伏的攻擊元件，並將情報傳送給分析、處理和鑑識小組。
- **調整性：**出現警示時，您可以根據攻擊方式進行調整，或是將資料收集、警示以及對攻擊目標的回應加以自動化，或者自訂組態以配合客戶的工作流程。
- **持續性：**偵測到攻擊事件時，永久的收集器會啟動觸發程序，對您和您監看的系統發出警示並通報攻擊活動。

不斷演化的威脅環境

企業已意識到他們可能隨時遭到攻擊者入侵，因此必須提早偵測到攻擊和進行中的活動，或是提早發現攻擊指標 (IoA)，才能做好有效應付這些入侵威脅的準備。有了這層認知後，企業也理解到他們需要新的技術，才能彌補目前在掌握、發現、偵測和回應等方面的落差。

目前事件回應方式的限制

當事件回應人員和安全性管理員奉命調查整個組織中的可疑或已知事件時，通常會受限於兩個關鍵因素：時間和規模。儘管現有的系統和工具可取得大量的詳細資訊，管理員卻需要花上很長的時間才能收集並分析這些資訊。由於速度是收集資料時最重要的條件，因此不但必須對所收集資料的性質做出重大讓步，收集的系統數目也連帶跟著減少。此外，光是針對收集到的資料重要性進行篩選，以分辨出重要資訊，就已經日益困難。

回應人員最常使用的事件回應工具，是他們自己撰寫的指令碼。這些工具提供收集資料的基礎，以應用在更廣泛的分析中。這項資訊體系以及相關工具的發展已經相當成熟，但若要大規模地快速運用，卻還力有未逮。由於無法對整個組織中的特定攻擊指標進行即時調查，經常讓回應人員在探索和回應問題時難以看清全貌。這些工作通常受限於必須符合時間要求的人為因素，而可能成為處理事件回應時的重大缺憾。這情況大大地妨礙了回應人員，因為他們的工作迫於目前工具的限制，受困於人為方面的阻礙。

全方位的端點偵測與回應

McAfee Active Response 能夠持續偵測及回應進階的安全性威脅，同時透過前瞻性探索、詳細分析、鑑識調查、全面性報告和排定優先次序的警示與動作，協助安全性從業人員監控安全性狀態、增進對威脅的偵測，以及提升事件回應能力。McAfee Active Response 已徹底改良以符合嚴格的端點偵測與回應 (EDR) 標準，並使用預先定義且可供使用者自訂的收集器來深入搜尋所有系統以找出攻擊指標，這些攻擊指標不僅在執行處理程序時存在，也可能潛伏在系統中，或甚至已被刪除。此外，McAfee Active Response 不但可讓使用者搜尋當下的攻擊指標，還可在未來萬一出現攻擊指標時，透過觸發程序的指令依據安全目標發出警示並採取行動。

整合性 McAfee 安全性架構的效能，可透過 McAfee Active Response 獲得實證，讓您可在更複雜的環境中，以更少的資源，更快速解決日漸複雜的威脅。McAfee Active Response 讓您能夠持續看見並深入洞悉您的端點，以加速確認入侵的威脅。它所附加提供的工具，也可讓您用最適合您企業的方式更快速地修正問題。這些所有的強大功能都是由 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體負責管理，此軟體採用 Data Exchange Layer，可以提供統一的延展性與擴充性，且不需要增加人手來管理產品。

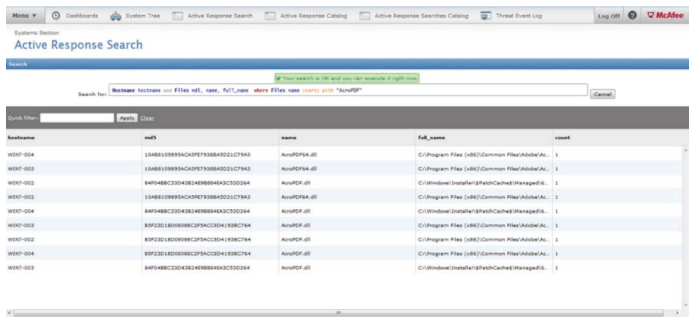

圖 1. McAfee Active Response 搜尋的使用者介面。

系統需求

最低硬體需求

如有必要，可將伺服器安裝於虛擬機器上。McAfee Active Response 伺服器的建議最低硬體需求如下：

- 4 Intel Xeon CPU X5675，3.07 GHz
- 8 GB RAM
- 120 GB 固態硬碟

所需服務基礎架構

- McAfee ePO 5.1.1 或更新版本
- McAfee Agent 延伸模組 5.0 或更新版本
- Data Exchange Layer 2.0.0.405 代理或更新版本

支援的 Web 瀏覽器

- Microsoft Internet Explorer 9 (含) 以上的版本
- Google Chrome 17 或更新版本
- Mozilla Firefox 10.0 或更新版本

所需用戶端基礎架構

- McAfee Agent 5.0.0.2710 或更新版本 (適用於 Linux 端點)
- McAfee Agent 5.0.0.2610 或更新版本 (適用於 Microsoft Windows 端點)
- Data Exchange Layer 2.0.0.405 用戶端或更新版本 (適用於所有受管理的端點)

支援的用戶端作業系統

- Microsoft Windows
  - Windows 8.0，Base，32 位元與 64 位元
  - Windows 8.1，Base，U1；32 位元與 64 位元
  - Windows Server 2012, Base，R2，U1；64 位元
  - Windows Server 2008 R2 Enterprise，SP1，64 位元
  - Windows Server 2008 R2 Standard，SP1，64 位元
  - Windows 7 Enterprise，最高 SP1，32 位元與 64 位元
  - Windows 7 Professional，最高 SP1，32 位元與 64 位元
- CentOS 6.5，32 位元
- RedHat 6.5，32 位元

功能	優點	客戶優勢	獨到之處
收集器	收集器可讓使用者尋找系統的資料並加以視覺化。	收集器提供搜尋功能，可更深入查看系統，並可讓您看到重大入侵和潛在攻擊，然後從這些系統收集資料並加以視覺化。使用者只要利用一些常見的指令碼語言，即可輕鬆自訂自己的收集器和回應，進而擁有最佳的設定性和調整性。	McAfee Active Response 能夠深入洞悉可執行檔及執行中檔案的程式碼，即使是潛伏在系統中的檔案，或攻擊者為了掩蓋蹤跡而刪除的檔案，也都將無所遁形。McAfee Active Response 可以搜尋檔案、網路流量、登錄項目和處理程序對應。
觸發程序	觸發程序可透過一組指令，讓安全性工作人員不論在當下或未來，都能持續監控重要的事件或狀態變更。	預先設定的觸發程序會採取適當動作，以產生事件或執行回應。McAfee Active Response 不僅有靜態的「透視」能力，還具備可持續回應的模式。	McAfee Active Response 能夠看見當下的威脅，並針對未來可能發生的威脅觸發相應的行動。
反應	達到觸發條件時，反應會提供預先設定和可供自訂的動作，讓您將所有威脅一網打盡。	反應讓使用者可以採取適當動作，例如搜尋系統中已由檔案雜湊 (MD5 和 SHA1) 刪除的檔案，查看主機目前是否與某個 IP 位址建立任何作用中的連線，或過去曾經建立連線；或者搜尋尚未經過存取或尚未在系統上爆發的非 PE 惡意檔案 (例如搜尋系統中已複製到檔案系統但尚未開啟的的惡意 PDF)。	McAfee Active Response 已預先設定為會針對搜尋結果做出反應，並採取使用者規定的自訂動作，以符合使用者定義的特定需求。
透過 McAfee ePO 軟體集中管理	單一主控台環境提供全方位的管理和自動控制。	管理員可以利用整合式 McAfee 安全性架構中的 McAfee ePO 軟體，針對觸發程序和搜尋結果自動回應，並回應和減輕威脅。在單一窗格進行管理提供了更好的安全可見性，無需增加額外的管理負擔。這可以簡化作業流程並減少管理人員的作業時間。	透過單一主控台即可管理和行動，是這項產品最大的特色。只要使用單一主控台，再搭配一組強大的安全控制項，包括 McAfee Active Response，就能為各種平台提供防護。
整合式安全性架構	運用資料交換層，簡化與其他 McAfee 旗下其他產品的通訊。	透過平台的創新概念、優化的流程和實用的建議，整合式 McAfee 安全性架構的 McAfee Active Response 不但可降低風險和回應時間，還可減少花費和作業人員成本。	

深入瞭解

深入瞭解 McAfee Active Response 的優勢：
www.mcafee.com/tw/products/active-response.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