

McAfee Database Activity Monitoring

具成本效益的資料庫防護，符合您法規遵循的需求



主要優點

- 徹底掌握所有攻擊來源並有效防護。
- 監視外部威脅、特權內部人員及來自資料庫內的複雜威脅。
- 在攻擊造成損害之前予以阻止，以降低風險並減少後續責任歸屬。
- 以更快的部署和更有效率的架構來節省時間與金錢。
- 讓您靈活地在所選擇的 IT 基礎架構上輕鬆部署。
- 與核心 McAfee 產品整合，例如 McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理平台和 McAfee Vulnerability Manager for Databases。

組織將最寶貴和機密的資料儲存在資料庫中，但資料庫隨附的周邊防護和基本安全性無法防止現今狡猾的駭客或潛伏內部的潛在威脅。研究1指出 96% 以上遭到入侵的記錄都與資料庫有關，其中 66% 的入侵長達數個月甚至更久都無人發現。McAfee® Database Activity Monitoring 會自動尋找網路上的資料庫、以預先設定的防禦來保護它們，並協助為您的環境建置自訂安全性原則，如此一來，不僅讓向稽查者證明法規遵循的工作變得容易，同時改進重要資料資產的防護。

透過 McAfee Database Activity Monitoring，組織可深入瞭解所有資料庫活動，包括本機的特權存取和資料庫內部的複雜攻擊。McAfee Database Activity Monitoring 可協助他們保護最寶貴和機密的資料，防堵外部威脅和帶惡意的內部人員。除了提供可靠的稽核追蹤，McAfee Database Activity Monitoring 還可終止違反安全性原則的工作階段來防止入侵。

McAfee Database Activity Monitoring 可協助組織：

- 快速建置自訂安全性原則來符合產業法規或內部 IT 管理標準。
- 記錄機密資料的存取情形以方便稽核，包括完整的交易詳細資料。
- 終止已違反原則的工作階段並隔離可疑的使用者，避免資料受到危害。
- 維持許多法規所要求的職責分離。

McAfee Database Activity Monitoring 以具成本效益的方式保護資料，防止所有威脅，可本機監視每一個資料庫伺服器的活動，並即時警告或終止惡意行為，即使在虛擬或雲端運算環境中執行也一樣。

阻擋所有資料庫威脅媒介

以資料庫中儲存的寶貴資料為目標的攻擊可能來自網路、來自已登入伺服器本身的本機使用者，甚至是來自資料庫本身透過預存程序或觸發事件所發動的攻擊。McAfee Database Activity Monitoring 採用非侵入式的單一解決方案，以記憶體型偵測器來攔截以上三種威脅。然後，此資訊可用來展現法規遵循以方便稽核，並改進組織最寶貴資料的整體安全性。

即時識別威脅，降低風險與責任

不同於基本的稽核或記錄分析，只在事後才告訴您發生的事情，即時監控和入侵預防功能可在漏洞造成損害之前防堵漏洞。警示會直接傳送至監視儀表板，提供原則違規的完整詳細資料，以利進行修補。可將高風險的違規設定為自動終止可疑的工作階段並隔離惡意使用者，預留時間讓安全小組調查入侵事件。

虛擬修補可防止已知入侵和許多零時差威脅

有時無法立即安裝廠商修補程式，因為其需要應用程式測試和停機時間來套用這些更新。此外，有些應用程式仍使用舊版的資料庫，但這些版本的修補程式卻沒有在提供了。McAfee Database Activity Monitoring 會偵測嘗試入侵已知弱點的攻擊和常見的威脅媒介，且可加以設定要即時發出警示或終止該工作階段。定期會提供新發現弱點的虛擬修補更新，且無須資料庫的停機時間就可實作，以在資料庫廠商發布可供套用的修補程式之前，保護機密資料。

使用最少資源，快速和非侵入地進行部署

McAfee Database Activity Monitoring 是純軟體的解決方案，可在一小時內完成實作並開始保護資料庫，不需要特殊的硬體或額外的伺服器。為進一步加速部署，McAfee Database Activity Monitoring 可自動掃描網路上的資料庫，並採用適合各種監控環境的精靈導向範本，引導使用者快速建立自訂的安全性原則，以符合稽核需求。McAfee Database Activity Monitoring 會將實作安全性原則的責任分散至在每一個資料庫伺服器上執行的自主偵測器，採取具成本效益的方式調整規模，以支援最大型的企業。

支援當今的現代化 IT 基礎架構，包括虛擬化和雲端

其他的資料庫監視系統需要仰賴網路流量的分析，才能識別原則違規，但對於資料中心虛擬化和雲端計算所用之高度動態及分散的架構而言，這是不可行或是沒有效率的方式。相較之下，可將

McAfee 偵測器設定為隨著每一個新的資料庫而自動供應，並根據伺服器所代管的資料而要求安全性原則，然後開始將任何警示傳送至管理伺服器。即使網路連線中斷，資料仍受到保護，因為偵測器會在本機實作安全性原則，並將警示會放入佇列中，等待再次連上管理伺服器時再進行傳送。

與 McAfee ePolicy Orchestrator 平台整合

McAfee Database Activity Monitoring 與 McAfee ePolicy Orchestrator 軟體完全整合，從統一儀表板提供所有資料庫的集中式報告和摘要資訊。McAfee ePO 軟體可與資料庫防護以外的其他 McAfee 安全性解決方案連接，藉此提供「單一窗格」檢視，以便輕鬆管理並有效全盤掌握。

McAfee 資料庫安全性解決方案

McAfee 提供了許多其他資料庫安全性解決方案，有助於全盤掌握整體資料庫狀況與安全性狀態。若要深入瞭解，請造訪 www.mcafee.com/tw/products/database-security/index.aspx，或連絡當地 McAfee 代表或附近的經銷商。

關於 McAfee 端點安全

McAfee 端點安全提供適合所有裝置使用的安全性措施，能保護透過裝置執行的資料及在其上執行的應用程式。全方位的特製化解決方案不但能降低多層式端點防護的複雜度，還能避免影響生產力。若要深入瞭解，請造訪 www.mcafee.com/tw/products/endpoint-protection/index.aspx。

