

# McAfee Application Data Monitor

透過應用程式層級檢查功能，有效偵測隱匿的威脅。

McAfee® Application Data Monitor 裝置可監視的範圍擴及應用程式層級，讓安全性與法規遵循不再侷限於記錄管理可及的範圍內。您可以完整檢查應用程式內容，以最深入的程度監看網路使用情形。

McAfee Application Data Monitor 裝置可解碼整個應用程式工作階段到「第 7 層」，讓基礎通訊協定、工作階段完整性，乃至於應用程式本身的內容（例如電子郵件文字或其附件）等所有項目，都可受到完整的分析。這樣的詳細程度不僅可精確分析實際的應用程式使用情形，也可讓您強制應用程式使用原則並偵測惡意、隱匿的流量。

此一深度檢查可追蹤網路上所有的敏感資料使用情形，而支援法規遵循工作。McAfee Application Data Monitor 裝置在偵測到違規時，將會保存該應用程式工作階段所有的詳細資料，以用於資安事件回應與鑑識工作，或用於法規遵循稽核需求。

同時，McAfee Application Data Monitor 裝置也可讓您發現可能偽裝成合法應用程式的威脅：

- 進階的應用程式層級威脅
- 未經授權使用或竊取敏感資料的行為
- 對安全死角發動的攻擊，或從安全死角入侵的攻擊
- 使用危險舊版程式碼的行為
- 竊取或濫用使用者認證的行為
- 透過任何應用程式傳輸敏感資料的行為
- 不健全的商業程序

## 資料遺失與法規遵循違規

McAfee Application Data Monitor 裝置可在機密資訊透過電子郵件附件、即時訊息、檔案傳輸、HTTP Post 或任何其他應用程式進行傳輸時加以偵測，並立即通知您以減少損失。

## 主要優點

- 可以對數以百計的應用程式，一路解碼整個應用程式工作階段到「第 7 層」
- 納入針對法規資料與敏感資料而預先建置的偵測規則
- 支援可由使用者定義的字典與規則，以提供自訂功能
- 產生應用程式事件的完整稽核追溯，以利進行法規遵循作業
- 被動操作，以避免干擾應用程式
- 與 McAfee Enterprise Security Manager 整合，讓應用程式內容能夠與事件和其他資料摘要產生關聯
- 彈性的混合式傳送選項，包含實體裝置與虛擬裝置

## 資料工作表

您可以透過現成可用的方法來偵測敏感資料 (例如信用卡資料與身分證號碼), 或自行定義重要與機密資訊的字典, 以自訂 McAfee Application Data Monitor 裝置的偵測功能。McAfee Application Data Monitor 裝置會偵測這些敏感資料類型、警示相關工作人員, 並記錄違規事項以維護稽核追溯。

### 文件探索

McAfee Application Data Monitor 裝置可在文件透過電子郵件、交談、P2P、檔案共用與其他途徑在網路上交換時, 探索超過 500 種類型的文件。McAfee Application Data Monitor 裝置在探索文件時, 無論副檔名為何均會進行探索, 即使將文件偽裝成其他類型, 企圖繞過郵件閘道與入侵偵測系統 (IDS)/入侵預防系統 (IPS) 裝置, 依然難逃法眼。即使是內嵌於其他文件中的文件, 以及封存、壓縮與編碼的文件, 也會經由檔案名稱與執行的操作等可行的度量被探索出來。

### 應用程式層級威脅

精密的新型威脅會入侵一般商用程式的弱點, 以滲透您的網路中並匯出敏感資料。這些應用程式層級威脅難以使用傳統的防火牆以及 IDS 與 IPS 偵測出來, 但 McAfee Application Data Monitor 裝置卻可深入查看應用程式所有的內容 (包括基礎通訊協定), 以偵測隱藏的承載、惡意軟體甚至隱匿的通訊通道 (例如 PDF 文件中內嵌的可執行檔)。

### 通訊協定異常

異常偵測可主動找出潛在的威脅, 以降低風險並壓低損失。部分傳統安全性解決方案限定於網路資料流的分析, McAfee Application Data Monitor 裝置則將此方法提升至更高的層級。我們依據過去的網路行為, 偵測應用程式與通訊協定內的異常, 提供更健全、更具主動性的風險偵測方法。

### 不干擾應用程式

McAfee Application Data Monitor 裝置是在 SPAN 連接埠上運作的, 因此不會干擾到應用程式的效能或可靠性, 或是造成延遲。

### 與您的基礎架構整合

大部分的網路監視解決方案多半是獨立運作的, 但 McAfee Application Data Monitor 裝置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, 損失和詐騙偵測功能將可與分析、網路檢查、資料庫事件監視等強大功能整合在一起。

### 使用案例

McAfee Application Data Monitor 裝置可偵測各種未經授權的活動、原則違規、竊取與詐騙。其範例如下。

### 支援的應用程式與通訊協定數量超過 500 個

- **低層級網路通訊協定:** TCP/IP、UDP、RTP、RPC、SOCKS、DNS 等
- **電子郵件:** MAPI、NNTP、POP3、SMTP、Microsoft Exchange
- **網頁郵件服務:** AOL 網頁郵件服務、Hotmail、Yahoo! Mail、Gmail、Facebook 與 MySpace 電子郵件
- **即時傳訊:** AOL、ICQ、Jabber、MSN、SIP 與 Yahoo
- **檔案傳輸通訊協定:** FTP、HTTP、SMB 與 SSL
- **壓縮與解壓縮通訊協定:** BASE64、GZIP、MIME、TAR、ZIP 等
- **封存檔:** RAR 封存檔、ZIP、BZIP、GZIP、Bin-hex 與 UU 編碼封存檔
- **安裝套件:** Linux 套件、InstallShield CAB 檔、Microsoft CAB 檔
- **影像檔:** GIF、JPEG、PNG、TIFF、AutoCAD、Photoshop、Bitmap、Visio、Digital RAW 與 Windows 圖示
- **音訊檔:** WAV、MIDI、RealAudio、Dolby Digital AC-3、MP3、MP4、MOD、RealAudio、SHOUTCast 等
- **視訊檔案:** AVI、Flash、QuickTime、Real Media、MPEG-4、Vivo、Digital Video (DV)、Motion JPEG 等
- **其他應用程式與檔案:** 資料庫、試算表、傳真、Web 應用程式、字型、可執行檔、Microsoft Office 應用程式、遊戲, 及軟體開發工具
- **其他通訊協定:** 網路印表機、殼層存取、VoIP 與點對點

### 竊取機密資訊

一名員工以 zhangsan@company.com 的身分登入，並傳送電子郵件至 lisi@gmail.com。電子郵件中包含名為 shoo.doc 的檔案，其中含有「秘方」一詞。此電子郵件於下午 12:20 從主機 desktop0232 (192.168.0.36) 透過 SMTP 伺服器 (10.0.2.13) 寄出，其主旨為：到手了。

### 在未經授權的情況下使用應用程式

一名員工使用自己安裝的點對點檔案共用應用程式傳輸音樂，而違反了原則。他在上班時間傳送了大量檔案，耗用了重要頻寬。據進一步調查顯示，這名員工是累犯。他不但使用 Jabber 與 IRC，並且在自己的桌上型電腦上執行未經授權的 Web 伺服器。

### 在工作場所上網摸魚

某名員工私底下是股票買方。她在上班時間連線至金融交易網站，平均上午和下午各花一小時。她也利用公司的 VoIP (SIP) 系統打電話，平均一天六通，並且在 Yahoo! Messenger 上使用「張三」的身分，花費數小時與「李四」和「王五」交談。

### 使用者採用弱式密碼

公司的安全性原則中，要求所有的使用者系統與應用程式帳戶均須使用強式密碼。Microsoft Active Directory 帳戶受到嚴密的管理。但在未使用 Active Directory 的對外 FTP 伺服器、郵件伺服器與關鍵的 Web 應用程式上，卻使用數十個弱式密碼。

### 深入瞭解

如需詳細資訊，請造訪我們的網站，網址為：[www.mcafee.com/tw/products/siem/index.aspx](http://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](http://www.mcafee.com/tw)

McAfee 和 McAfee 標誌皆是 McAfee, LLC 或其附設公司在美國及其他國家地區的商標或註冊商標。  
Copyright © 2017 McAfee, LLC.  
61322ds\_app-data-monitor\_0914  
2014 年 9 月