

Trellix Data Loss Prevention Monitor

保護重要資料

保護客戶和員工的個人隱私資料 (包括身分證號碼、信用卡號碼或其他個人資訊等) 是現今每個人深知的重點。因員工疏失、筆記型電腦遺失以及遺忘 USB 裝置而導致資料意外洩漏,幾乎是所有組織都會面臨到的安全性挑戰。除此之外,當資料透過 Google Gmail、Yahoo! Mail、即時傳訊以及 Facebook 等 Web 應用程式傳輸及分享時,就有可能洩漏資料或落入他人手中。Trellix Data Loss Prevention Monitor (Trellix DLP Monitor) 是一項高效能資料遺失防護解決方案,可以分析所有網際網路通訊內容,並判定資訊是否誤傳至他處,協助您盡可能降低安全性團隊的工作量、符合法規要求,並保護智慧財產權和其他重要資產。

監控、追蹤傳輸中的資料並提出報告

不論業務類型為何,您都需要能識別透過任何應用程式、任何通訊協定、任何連接埠、及任何形式傳送之敏感資訊的可見性,同時還必須兼具高度的準確度。

有了 Trellix DLP Monitor 之後,您可以即時收集、追蹤在整個網路中傳輸的資料並提出報告,因此能尋找有哪些資訊透過哪些方式在使用者與其他組織間流動。Trellix

DLP Monitor 是一款高效能、以目標為導向的裝置,它特別能偵測出超過 300 種在任何連接埠或通訊協定上週遊的內容類型,因此能協助您揭露資料所面臨的威脅,以及採取動作來

協助組織預防資料遺失。此外,Trellix DLP Monitor 還能透過一般使用者通知來教導使用者瞭解何謂資料遺失違規,以在不費吹灰之力的情況下改變行為。

即時掃描及分析資訊

Trellix DLP Monitor 能使用 SPAN 或 Tap 連接埠而整合至網路中,執行網路流量的即時掃描與分析。憑藉著超過 150 個 範圍涵蓋法規遵循與智慧財產之合理使用方法的預建規則,Trellix DLP Monitor 能將文件的完整或部分內容 (包括極小部分的抄襲) 與全面的規則集進行比對。這可讓您偵測網路流量中的異常狀況,不論大小規模為何。

主要優點

- 識別及保護敏感資訊:
 - 透過直覺式的搜尋引擎快速識別敏感資訊。
 - 實施鑑識分析以使現在與過去的風險事件相互關聯、偵測風險趨勢及識別威脅。
 - 立即建立規則以預防未來的行為。
- 透過 Trellix ePolicy Orchestrator[®] (Trellix ePO™) 軟體達到完全統合。
- 透過 Trellix ePO 軟體進行完整的管理,因此可與 Trellix DLP Endpoint 共用通用的原則管理、事件管理和案例管理,並建立及調整精密的規則。
 - 識別超過 300 種透過任何連接埠與應用程式傳送的獨特內容類型。
 - 跨越連接埠的限制將網路流量分類。
 - 能予以擴充以支援數十萬個同時連線。

深入探討未曾考量過的風險

經由詳細地分類、索引及儲存所有網路流量（不僅只是符合即時規則的資訊），Trellix DLP Monitor 能讓您快速運用歷程資訊來瞭解哪些資料是敏感資料、資料的使用情況、資料的使用者及資料移動的目的地。此外，您還可以執行鉅細靡遺的調查與資訊歷程檢查，以偵測出先前未曾考量過的風險事件與資料揭露。搭配 Trellix DLP Discover 一同部署後，您亦可識別資料在網路中的儲存位置與資料的擁有者。

檢視事件報告以提供動作參考資訊

當 Trellix DLP Monitor 使用分類引擎來掃描、分析及分類流量後，它會將所有相關資訊存放在專屬的資料庫中。您可以使用直覺式的搜尋介面來檢視完整的報告以獲得所需的資訊（包括傳送者、目的地、傳送方式），因此可以判斷出外洩的資訊為何、從哪裡外洩，以及如何外洩。得知這些情報後，您可以套用一系列的動作來解決這些威脅，進而維護法規遵循及保護敏感資料。

規格

系統輸送量：以高達 200 Mbps 的速度分類內容（無取樣）

網路整合：能使用 SPAN 連接埠或實際內連的網路 Tap（選用）以被動方式整合至網路中

支援超過 300 種內容類型的檔案分類，包括：

- Microsoft Office 文件
- 多媒體檔案
- P2P
- 來源碼
- 設計檔案
- 封存檔
- 加密檔案

將各種資料分類

Trellix DLP Monitor 能讓您的組織掃描所有類型的敏感資料，不論是常見的固定格式資料，或是複雜且型態不一的智慧財產，均可加以審視。藉由合併這些物件分類機制，Trellix DLP Monitor 能建置精準度高且詳細的分類引擎，並運用引擎來篩選敏感資訊及執行可識別隱藏或未知風險的搜尋。

物件分類機制包括：

- **多層式分類：**以階層格式涵蓋內容相關資訊與內容
- **文件註冊：**包括資訊變更時的生物識別特徵碼

- **文法分析：**偵測文字文件、試算表或原始程式碼等所有內容中的文法或語法
- **統計分析：**追蹤特定文件或檔案中出現與特徵碼、文法或生物識別相符之項目的次數
- **檔案分類：**跨越檔案或壓縮檔的副檔名限制，識別內容的類型

機型與裝置選項

Trellix DLP Monitor 以硬體或虛擬裝置的形式提供。如需詳細資料，請參閱 [Trellix DLP 6600 硬體裝置資料工作表](#)。

規格 (接上頁)

支援的通訊協定

- 支援所有透過任何通訊協定或將 TCP 當做傳輸通訊協定之連接埠的傳輸。
- 包括 HTTP、HTTPS、SMTP、IMAP、POP3、FTP、Telnet、Rlogin、SSH、網頁郵件服務、Yahoo! Chat、AOL Chat、MSN Chat、ICY、RTSP、SOCKS、PCAnywhere、RDP、VNC、SMB、Citrix、Skype、IRC、LDAP、DASL、NTLM、Kazaa、BitTorrent、eDonkey、Gnutella、DirectConnect、MP2P、WinMX、Sherlock、eMule 等的通訊協定處理常式

內建原則

- 提供多種適用於共同需求的內建原則與規則，包括法規符合性、智慧財產及合理使用方法等
- 您可以運用 Trellix 擷取資料庫來完成徹底的規則自訂化，以滿足業務的特定需求



Trellix 和 Trellix 標誌皆是 Musarubra Singapore Pte Ltd 或其附設公司在美國及其他國家/地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。