*** 由於業務的性質，本故事中出現的組織名稱將保持匿名。**

探索 OPSWAT MetaDefender Core 多防毒引擎掃描技術，如何為保險業的檔案上傳安全提供支援，防止惡意軟體和資料洩露。

根據 IBM發佈的一份報告，截至2022年底，全球資料洩露的平均成本達到445萬美元，在過去三年中大幅增長了15%。為了應對這些令人震驚的統計資料，51%的組織傾向於在遇到漏洞後，加強對資訊安全的投資。他們著重於加強事件響應計劃，提供全面的員工培訓，並加強其威脅檢測和回應能力，以減輕未來風險。

本案例中，這家保險經紀公司管理著近160億美元的風險溢價，並在美國各地擁有龐大的辦事處網路，保護敏感資料成為其絕對的優先事項。他們的解決方案是什麼？ OPSWAT MetaDefender Core，以下我們將深入探討這家公司面臨的現實挑戰，探討他們為什麼選擇 MetaDefender Core，並揭曉他們取得的顯著成果。

為什麼保險經紀公司會成為攻擊目標?

由於保險經紀公司處理大量敏感和有價值的資訊，是檔案上傳安全相關網路威脅的主要目標。這些企業經常管理大量的個人和財務資料，包括投保人的個人詳細資訊、醫療記錄和財務記錄，使其成為身份盜竊、詐欺或其他惡意活動的網路犯罪分子的寶庫。

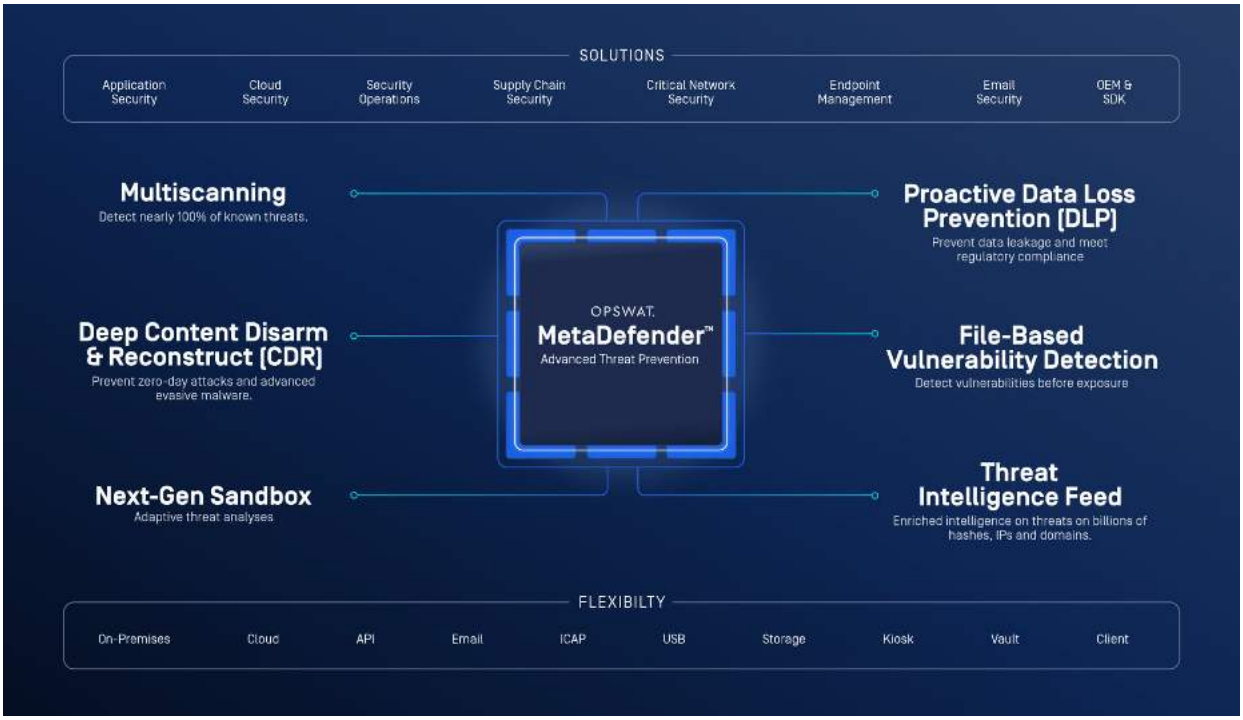
保險業數位檔案傳輸的便利性，使得威脅行為者更容易利用檔案上傳系統中的漏洞，從而可能導致資料洩露和經濟損失。在這個具體案例中，這家保險經紀公司在全國範圍內營運，在美國數百個辦事處擁有數千名專業人員。

在管理如此廣泛的網路時，他們遇到了幾個重大挑戰：

- **無處不在的惡意軟體：** 從客戶、索賠人、代理商和其他來源收到的檔案數量不斷增加，使其電腦系統面臨惡意軟體感染的風險。
- **法規合規性：** 為了遵守 Gramm-Leach-Bliley Act (GLB), Sarbanes-Oxley Act (SOX), Federal Insurance Security Management Act (FISMA) 等政府規定，該公司需要一個有效的反惡意軟體解決方案。
- **時間和成本問題：** 解決與惡意軟體相關的問題會耗費寶貴的時間和資源，促使該公司想要找可以簡化此流程的解決方案。

更高級別的檔案上傳安全性

在尋找強大的網路安全解決方案時，該公司求助於 OPSWAT。



MetaDefender Core 被經紀公司選為檢測和防止病毒、蠕蟲、木馬等惡意軟體進入其資訊網路最有效的方法。整合多防毒引擎掃描技術和八個內建防病毒引擎，MetaDefender 能在公司接收這些檔案之前，徹底掃描檔案中的惡意軟體。

MetaDefender Core 還包含客製化發佈操作等功能，使經紀公司能夠控制流入其網路的資料流程。使用這些客製化發佈操作，經紀公司建立了以下資料流程：立即隔離受感染的檔案，並通知寄件者檢測到惡意軟體。接著請求寄件者重新提交乾淨的檔案，並刪除受感染的檔案。

結果

MetaDefender Core 為保險經紀公司取得了以下成果：

- 惡意軟體防護

自從使用MetaDefender 以來，該公司並未回報任何與惡意軟體相關的檔案問題。

- 法規合規性

OPSWAT 幫助公司保持合規性，滿足政府嚴格的法規，確保敏感財務資料的安全。

- 降低成本

公司不再需要分配大量 IT 資源來修復惡意軟體相關事件。

確保保險資料安全

保險經紀公司與 OPSWAT和MetaDefender Core 的合作，是採取主動措施如何保護組織的一個成功案例。

透過優先考慮安全性、合規性和效率，這家公司鞏固了其作為保險行業領導者的地位，證明保護資料和營運，是當今數位世界的戰略要務。

如需進一步了解 OPSWAT的 MetaDefender Core 可以如何使您的組織受益，請立即聯繫專家。