# 金融業資安需求不斷攀升！

# 台灣知名銀行如何利用OPSWAT技術

# 降低惡意軟體威脅並確保檔案傳輸安全

銀行、金融服務和保險業（BFSI）最近面臨不斷升級的網路威脅，這些威脅正是利用檔案處理和資料傳輸的漏洞。

## BharatPay 資料外洩

2022 年，BharatPay 這家為印度客戶和商家提供各種數位金融服務的金融科技公司，發生了嚴重的資料外洩事件；由於資料處理作業出現了安全漏洞，導致約 37,000 名使用者的個人和交易資料在線上曝光。

## LockBit 贖金軟體攻擊

同樣地，在 2023 年 5 月，東南亞的一家國有銀行也成為 LockBit 贖金軟體群組的受害者，該群組透過外洩的憑證存取銀行網路，而造成大量資料外洩。

## Cosmos銀行網路騎劫案

另一個最近的例子是 Cosmos Bank 網路騎劫案，駭客透過跨 28 個國家的協調攻擊，揭露了銀行檔案與資料處理協定的漏洞，從中盜取 1,350 萬美元。

這些事件突顯出銀行、金融服務和保險業界檔案管理安全的重要性。未經驗證的上傳、不安全的檔案交換，以及對可攜式媒體的依賴，都會帶來巨大的風險，讓網路威脅更容易繞過傳統的防禦措施進入關鍵網路。金融機構現在需要能夠主動偵測並調和威脅，同時簡化檔案處理安全的解決方案，以保護客戶資料並維持信任。

本篇客戶故事將探討一家服務國內外數百萬客戶的台灣知名銀行，如何透過整合OPSWAT的 MetaDefender Managed File Transfer (MFT) 和 MetaDefender Core這些先進的安全解決方案，加強了對檔案型威脅的防禦，保障了營運和敏感客戶資訊的安全。

## 檔案管理的風險不斷增加

該銀行意識到網路威脅不斷進化，因此決定審慎評估其處理檔案傳輸的方法，並發現了現行的檔案傳輸辦法存在數個安全漏洞。尤其是依賴USB 進行內部檔案傳輸，會使銀行暴露於潛在的資料洩漏和惡意軟體風險中。若是沒有有效的方法來追蹤和驗證USB 的檔案傳輸，銀行就會面臨敏感資料外洩和外部威脅的風險。

「我們仰賴USB進行內部傳輸，導致檔案處理程序出現重大漏洞。因為USB缺少適當的安全檢查機制，惡意檔案進入我們的網路，或資料意外洩漏的風險一直存在。」——IT安全經理

此外，該銀行還遇到未經驗證的檔案上傳問題，尤其是在需要客戶提交大量檔案的國家紓困方案期間。由於沒有機制可驗證這些上傳的檔案是否安全，銀行的系統面臨了惡意軟體感染和未經授權存取的風險。如何安全地處理這些檔案已成為當務之急，尤其是該銀行已意識到潛在資料外洩對其聲譽和營運管理所造成的影響。

最後，組織內部頻繁的人事變動也帶來了額外的資料安全挑戰。透過手動方式在各部門間傳輸檔案的效率很低，敏感資訊可能會在傳輸過程中暴露而造成合規性風險。因此，該銀行需要一套能在不中斷日常運作的情況下，安全地將這些檔案交換自動化的解決方案。

您的企業也有檔案傳輸安全的需求嗎？現在就預約免費諮詢！

## OPSWAT 被該銀行選為保全檔案管理的系統，並協助銀行遵從法規

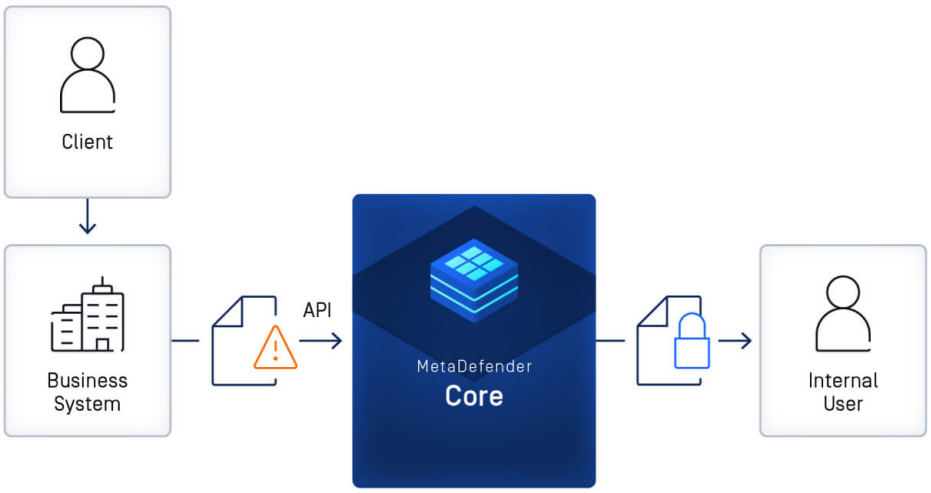
為解決這些重要挑戰，該銀行評估了各種網路安全解決方案，最後選擇了OPSWAT的 MetaDefender Managed File Transfer (MFT) 和 MetaDefender Core。OPSWAT的解決方案提供安全、檔案處理自動化與進階威脅偵測的獨特組合，讓銀行能同時處理內部與外部的資料風險。MetaDefender Core 和MetaDefender MFT 的本機整合提供了無縫的掃描方式，在每個傳輸檔案的地方都進行掃描，以確保全面地端對端安全性。

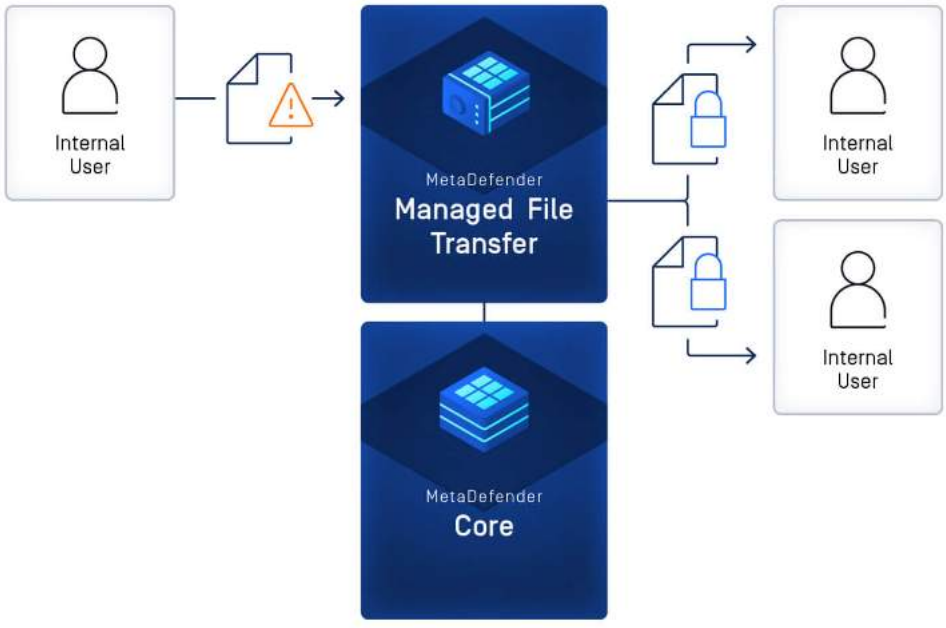

- **進階惡意軟體掃描：** MetaDefender Core 利用 Multiscanning與多防毒引擎掃描和 Deep CDR （檔案無毒化）來淨化檔案，在保存內容的同時，移除潛在的有害元素。
- **端對端加密：** MetaDefender MFT 在傳輸中和靜止狀態下都可以加密資料，確保檔案在整個傳輸過程中保持安全。
- **自動化工作流程：**透過自動化檔案傳輸流程，MetaDefender MFT 可消除手動處理的錯誤，並減少對不安全USB 裝置的依賴。
- **合規性與稽核追蹤：**這兩種解決方案都透過詳細的稽核記錄、角色式存取控制（RBAC,role-based access control）和回報功能，支援符合法規的標準。

「有了OPSWAT的解決方案，我們終於有了安全可靠的方式，來管理外部進入和內部傳輸的檔案。MetaDefender Managed File Transfer 和MetaDefender Core 為我們提供了主動管理威脅，和減少人為干擾的工具，讓我們的流程更安全、更有效率。」——IT 安全經理

## 加強人員輪調的檔案安全性

使用MetaDefender Managed File Transfer 的立即可見的效益之一，就是能夠在人事輪調時可以安全地管理檔案傳輸，而無需使用USB 。過去，銀行員工在輪調各部門、各分行時，會依賴USB 來傳輸必要的檔案，而造成有資料外洩的機會。現在，有了MetaDefender MFT 的安全自動化平台，員工可以在各部門間無縫地上傳和下載檔案。



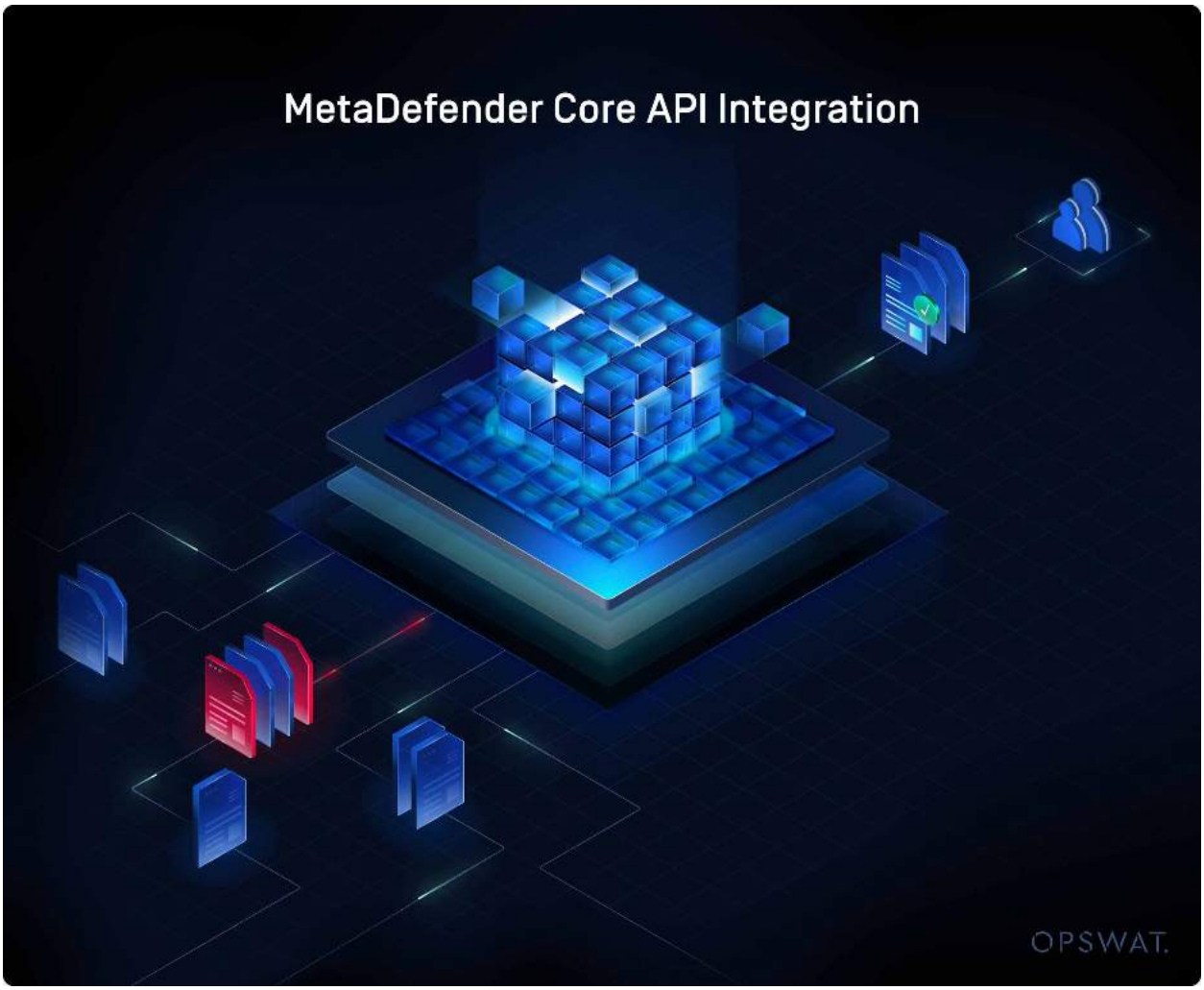




集中式的MFT 平台消除了手動處理裝置的需求，讓銀行能嚴格地控制存取權限。該解決方案基於角色的權限管理方式，可確保只有有授權的人員才能存取和傳輸特定檔案，大幅

降低了意外或故意洩漏資料的風險。安全的傳輸程序不僅提高了效率，還透過提供所有檔案移動的透明稽核追蹤，加強了銀行對業界法規的遵循。

**使用MetaDefender Core API 保護客戶的檔案上傳安全**

MetaDefender Core 應用程式介面 (API)，成為該銀行處理未經認證的客戶上傳檔案策略的根基。該銀行將API 與其業務系統整合，以掃描所有傳入的檔案，確保每份檔案在進入內部系統之前都經過嚴格的安全檢查。此解決方案在大規模的紓困計畫檔案提交時特別有作用，否則傳入的檔案可能會帶來惡意軟體風險。




透過Deep CDR 技術，MetaDefender Core 解除潛在的有害檔案內容，除去內嵌的威脅，同時保留原始資料。Multiscanning （多防毒引擎掃描）技術，針對已知和未知的威脅提供全面的防護，進一步提升偵測精確度。

「MetaDefender Core API 整合讓我們能夠安全地處理上千份傳入的檔案，因為我們知道這些檔案都經過徹底的掃描及消毒。即使在檔案提交高峰期，這項整合也能幫助我們維持運作的完整性，並保護客戶的敏感資料。」——IT 安全經理

## 改造系統更新和文件安全性

除了管理客戶上傳之外，OPSWAT的解決方案還簡化了銀行的內部流程，包括安全處理系統的更新和敏感的檔案傳輸。包含證書、軟體更新和其他關鍵資訊的檔案透過 MetaDefender Core API 整合進行消毒，在進入網路之前消除任何潛在威脅。此掃描程序，可以確保即使是例行更新，也能遵守銀行嚴格的安全標準，將意外感染惡意軟體的風險降至最低。

有了自動化的工作流程，銀行在處理敏感檔案時不再仰賴人工干預，更新速度更快、效率更高。MetaDefender MFT提供集中控制的監控儀表板，讓銀行的 IT 團隊能夠即時監督所有檔案移動，為內部作業增添另一層安全性。

## 透過稽核與控制達到合規標準

在受高度監管的金融業，該銀行必須確保其檔案管理實務符合資料保護和網路安全標準。MetaDefender MFT幫助該銀行的詳細紀錄稽核過程和基於角色的存取控制，讓該銀行能輕鬆滿足這些要求。透過產生報告和維護所有檔案傳輸活動的全面記錄，銀行可以在法規稽核時拿出證明有符合規定。

MetaDefender MFT靈活的部署選項，全面支援銀行的 297 家分行，讓銀行能在整個網路都實施一致的安全政策。此擴充能力可確保每家分行不論位於何處，都能遵守相同的高安全標準。該銀行的領導階層現在可以放心地管理資料處理程序，並迅速回應任何合規性查詢，加強該機構對遵守法規的承諾。

## 一個安全又高效的數位轉型方案

在實施MetaDefender MFT 和MetaDefender Core 六個月後，該銀行報告其網路安全和作業效率有顯著的改善。銀行數位基礎架構的惡意軟體威脅大幅降低，這要歸功於MetaDefender 解決方案的主動掃描和清除功能。透過改變基於USB 的檔案傳輸方式，該銀行也大幅降低了資料洩漏的風險，並簡化了內部流程。

- **減少資料外洩**

MetaDefender MFT 取代USB 裝置進行人員傳輸，大幅降低敏感資訊外洩的風險。基於角色的權限可提供進一步的保護，確保只有授權使用者才能存取特定檔案。

- **提升營運效率**

MetaDefender MFT自動化檔案處理工作流程將人工介入的需求降至最低，從而騰出 IT 資源處理其他任務。現在，系統更新和客戶檔案提交的處理既安全又高效，只需最少的人工參與。

- **改善合規性的資料準備流程**

有了強大的稽核和報告工具，銀行可以隨時證明自己符合業界標準。MetaDefender MFT 詳細的日誌，記錄確保了透明度和問責性，使銀行能夠迅速回應審計要求和監管規定。

- **改善傳入檔案的威脅偵測**

透過將MetaDefender Core 的API 整合至其業務系統，掃描所有傳入的檔案，該銀行大幅提升了偵測和中和惡意軟體的能力。這種前瞻性的方法，降低了檔案型威脅進入網路的風險，為敏感的客戶資料提供了更高的安全性。

- **簡化客戶檔案處理流程**

MetaDefender Core的自動檔案掃描功能，可確保客戶上傳的每份檔案都經過徹底檢查，無需手動介入。此自動化流程可讓銀行快速、安全地處理大量的客戶上傳的檔案，提高作業效率並減少人為錯誤。

「有了MetaDefender MFT 和MetaDefender Core，我們的網路系統不僅更安全，處理資料的方式也更有效率。這些解決方案讓我們得以不僅是被動的安全防護，可以採用主動、簡單的方式來處理網路安全。」——IT 安全經理

## 為金融機構樹立檔案管理安全的新標準

OPSWAT的MetaDefender MFT 和MetaDefender Core 的使用，重新定義了銀行的檔案管理和安全方法。透過改善未經認證的上傳、基於USB 的傳輸方式以及內部檔案交換等特定挑戰，該銀行已為金融業的資料安全性樹立了新基準。OPSWAT的解決方案讓銀行能夠安全地管理資料、維持合規性，並有信心面對不斷演變的網路威脅。

對於這家台灣的銀行而言，MetaDefender 解決方案不僅是工具，更是彈性網路安全架構的重要組成部分。本案例突顯了全面、安全的檔案管理解決方案所帶來的決定性影響，讓金融機構在日益複雜的數位世界中，能夠安心專注於成長與創新。

您的企業也有檔案傳輸安全的需求嗎？現在就預約免費諮詢！

看更多金融業的客戶成功案例：

**OPSWAT 解決了歐洲著名銀行檔案上傳安全的風險**

**台灣知名金控採用OPSWAT邊際防護與郵件安全解決方案來抵禦新式檔案型APT攻擊**