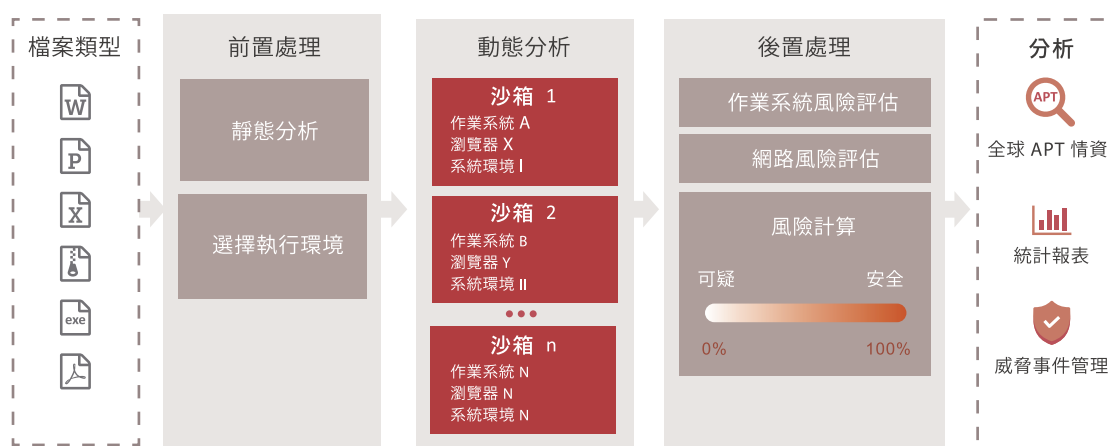


Openfind™ MailGates APT 動態沙箱分析解決方案

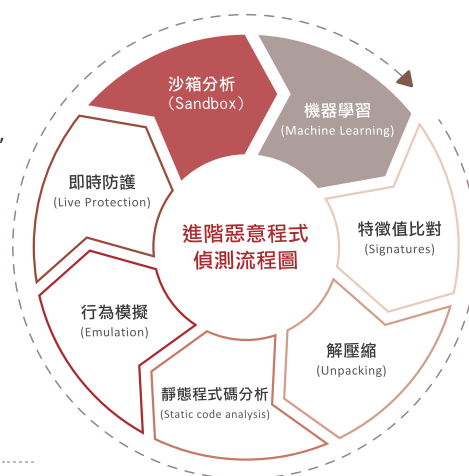
結合全球威脅情資系統 阻擋進階惡意郵件攻擊

近年 APT 攻擊事件猖獗，無論是惡意郵件、勒索病毒或是釣魚信件的威脅與日俱增，其中受害產業又以金融、製造及政府為駭客的首要目標，且普遍以電子郵件做為網路攻擊的前奏，進而入侵至企業網站達到目的。儘管駭客攻擊手法不斷變化更新，但多數企業用戶仍得仰賴電子郵件作為正式溝通管道，有鑑於此，Openfind MailGates 郵件防護系統推出 APT 動態沙箱分析解決方案，整合全球威脅情資 (Threat Intelligence)、靜態程式碼分析 (Static Code Analysis) 及動態沙箱分析 (Sandbox Analysis) 等多項防護機制，以透過機器學習模型解析檔案特徵，可攔截最新型態病毒及加密病毒信攻擊，大幅提升進階惡意程式的偵測率，有效降低被駭風險。



動態沙箱分析引擎 郵件安全防護全面升級

MailGates APT 防禦解決方案透過動態沙箱分析功能，協助企業過濾進出郵件，利用進階惡意程式偵測引擎，先比對信件附檔的特徵值，再將其解壓縮進行靜態程式碼分析並模擬檔案行為，判斷其是否為可疑檔案，接著查詢即時防護病毒資料庫，最後提交至被隔離的沙箱環境引爆，監控其行為並回傳詳細的分析報告，經客戶端實測結果證明，平均每日揪出 4% 具 APT 攻擊的郵件並成功將其隔離。



產品效益



精準過濾攔截 嚴密守衛滴水不漏

- URL 解析，剔除釣魚信、廣告信網址
- 獨家自動白名單機制，提升過濾精準度



動態沙箱分析引擎，阻攔進階惡意程式攻擊

- 動態沙箱模擬，將檔案提交至沙箱環境模擬執行
- 圖形化威脅報表，列出最具威脅使用者與檔案類型



深度學習偵測引擎 平均分析少於 120 秒

- 透過機器學習機制提高判別準確性
- 整合全球 APT 情資查詢服務



與安全電子郵件閘道無縫整合

- 可與 MailGates 電子郵件防護系統和 MailAudit 電子郵件稽核系統無縫整合
- 可過濾垃圾郵件、抵禦勒索病毒與未知惡意程式

FAQ

Q1 為什麼傳統防禦措施不能保護企業免於遭受 APT 攻擊？



基於特徵值 (Signature) 的防毒引擎只能偵測已知的病毒特徵, 且越來越多的惡意程式無法透過防毒引擎掃描出結果。大多數安全領導廠商使用進階的方式, 例如沙箱分析來彌補傳統防毒引擎的不足。

Q2 APT 動態沙箱分析有哪些檢查機制？



1. 全球威脅情資(Threat Intelligence), 有效阻擋零時差(Zero-Day)攻擊。
2. 靜態程式碼分析(Static Code Analysis), 透過機器學習模型解析檔案特徵, 可攔截最新型態病毒攻擊。
3. 動態沙箱分析(Sandbox Analysis), 支援全系統模擬(Full-system emulation)、規避型惡意程式偵測(Evasive Malware Detection)等機制, 可防止反沙箱病毒。

Q3 檔案被提交到沙箱分析前做了哪些檢查？



並非所有檔案都會送到沙箱。在上傳檔案進行分析之前, 需要執行多個檢查步驟：

1. 防毒引擎使用多種技術掃描檔案, 檢查是否有符合病毒的特徵值。檢查結果可分為安全、惡意或可疑。
2. 已知的惡意檔案會被隔離, 已知的安全檔案會發布給終端用戶。
3. 對於可疑檔案, 進階惡意程式偵測引擎將確定檔案是否包含任何可疑內容(例如 Office 檔案中的巨集或 PDF 中的 JavaScript)。
4. 若該檔案含可疑內容, 則將該檔案上傳到沙箱引爆並作進一步的分析。如果分析結果是惡意的, 則該檔案將被隔離。如果是安全的, 檔案將發布給終端用戶。

Q4 APT 動態沙箱分析解決方案支援哪些檔案類型？



以下列出支援的檔案類型

- PE 和 EXE 檔案, 包含 32 或 64 位元的 DLL 檔與執行檔
- Microsoft Office Word 檔 (副檔名為 .doc, .docx, .docm, .rtf)
- Microsoft Office Excel 檔 (副檔名為 .xls, .xlsx, .xlsm)
- Microsoft Office PowerPoint 檔 (副檔名為 .ppt, .pptx, .pptm)
- PDF 文件(.pdf) 及 PDF XML 文件(.xpf)
- ActiveMime
- 壓縮檔(ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, XZ)

支援郵件系統

Mail2000 | Microsoft Exchange | IBM Notes | Sendmail | Postfix

支援郵件雲端服務

Google Workspace | Microsoft 365 | Exchange Online

用戶端建議需求

Microsoft Edge | IE 11 | Firefox 最新版 | Chrome 最新版

網擎資訊軟體股份有限公司

10359 台北市大同區重慶北路二段 243 號 7 樓

TEL : (02) 2553-2000 分機 713 蔡小姐

FAX : (02) 2553-0707 客服專線:(02) 2553-7272

E-mail : info@openfind.com.tw | <https://www.openfind.com/>

授權經銷商