SOPHOS
Security made simple.

# Cloud-Based Sandbox雲端沙箱

## 透過動態惡意軟體分析來強化病毒防護

SOPHOS新世代沙箱平台整合了進階型的惡意軟體模擬分析，
藉以提供更妥善的解決方案。SOPHOS雲端沙箱擁有強大且含高擴充性的環境，
以針對未知或可疑程序和檔案進行深入嚴密的分析。
SOPHOS沙箱可透過其發布的API輕鬆整合到任何訊息和網頁安全產品中，
並且包括做為預先過濾的SOPHOS AV SDK，
有效降低實行進階威脅偵測系統相關的成本和複雜性。

### 優勢特點

- 適用於未知惡意軟體和零時差病毒的進階偵測
- 易於整合廣泛的使用案例和商務模式
- 能彈性保護任何大小的網路
- 簡易靈活的授權能實現最具成本效益的整合
- 強大的預先過濾和建立邏輯能確認需要進階偵測的檔案

### 趨勢的洞察力

隨著網路罪犯不斷研發難以捉摸的新型惡意軟體，讓感染成本也日趨複雜。零時差惡意軟體不但已比過往更加風行，還會針對已知的安全技術和防護進行規避。

想要開發出進階惡意軟體的安全解決方案，是必須經過複雜龐大的研發制定過程，以釐清那些檔案需要沙箱分析，以取得進階偵測、用戶體驗和財務預算等三方面的平衡。

SOPHOS沙箱能允許安全防護廠商輕鬆快速部署全面化的解決方案。其基礎是獨特的偵測平台，以SOPHOS屢獲殊榮的惡意軟體防護為輔，並與SOPHOS Labs威脅情報緊密結合。

### 專注於簡易整合和深度偵測的成熟技術

SOPHOS沙箱至今已來到第四代，被內部運用在獲獎肯定的SOPHOS產品有近十年之久。結合了最新的威脅分析以及強大模擬工具，以確保檔案偵測是使用即時情報以及廣泛的偵測技術。

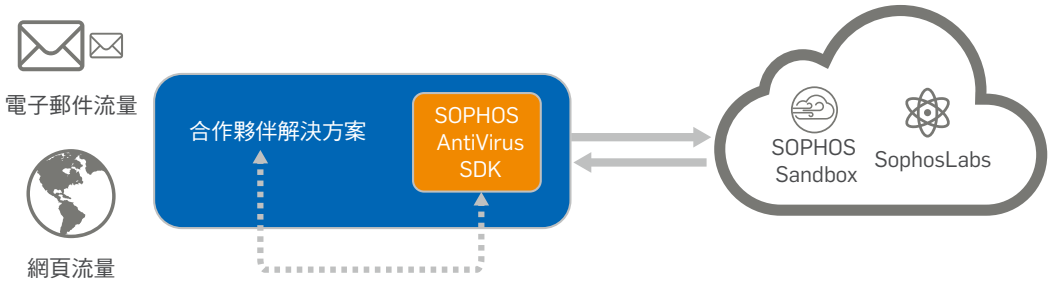
透過API和SOPHOS Antivirus SDK進行整合，可以讓安全廠商以最有效的方式為廣泛的使用案例部署沙箱功能，從而節省大量時間和資源，並消除人為錯誤的可能性。

### 進階偵測分析

SOPHOS Antivirus SDK擴充了雲端沙箱，以做為一個更有效的預先過濾功能，不僅設下第一道防線，也協助減少發送進階分析的誤報檔案數量。如此一來就可以實現最佳效能、提升用戶體驗、並加快對可疑檔案的分析。

## Cloud-Based Sandbox雲端沙箱

SOPHOS Threat Intelligence lab支援進一步的偵測功能，因為其提供透過SOPHOS同步安全所取得的資料：來自端點和網路安全設備的雙重分析，以實現一個更廣泛的分層式安全解決方案。




## 強化偵測&降低風險

SOPHOS沙箱能偵測零時差威脅和複雜攻擊，提供風險評等和攻擊修復所需的細項資訊。
然後，安全防護廠商可以運用這些偵測結果來觸發預防措施，以確保用戶安全，直到完成修復為止。

## 整體持有成本最低化

SOPHOS沙箱不僅提供先進的偵測功能，同時也維持低成本開支：

- 強大的預先過濾偵測和建立邏輯能立即分類大多數的檔案。
  隨著較少的檔案發送到雲端沙箱，頻寬成本將可保持在最低狀態。
- 易於整合和平台擴充性使安全防護廠商能夠更快獲得收益。
- 透過採用戶數、無檔案限制的訂閱模式，將能實現可預期的成本架構。

## 重點功能

| | |
|---|---|
| Pattern-based**偵測** | 協助發現惡意檔案和URL，包括其他偽裝威脅設計的針對性攻擊 |
| **惡意軟體規避防護** | SOPHOS沙箱可偵測惡意軟體的規避行為，<br>也能防範其他常見的記憶體漏洞攻擊，例如，記憶體堆疊噴濺攻擊（heap spray） |
| Pattern**自動更新** | 確保防護持續性和最大效能，以應對快速發展的進階威脅 |
| **精細判定** | 透過分析安全環境中的威脅，為可疑網站、檔案、應用程式和事件提供明確依據 |
| **與**SOPHOS Global Threat intelligence**整合** | 透過全球客戶經驗資訊，取得全面化的威脅情報 |

如您對SOPHOS想瞭解更多，或進一步需求，歡迎洽詢**湛揚科技**，
我們有專業資安團隊提供您詳細產品簡報，產品免費測試，讓您快速體驗SOPHOS強大有效的防護能力！

T-tech 台灣專業代理商 湛揚科技 www.t-tech.com.tw
110 台北市信義區基隆路二段109號10樓 | TEL：(02)2735-3512 | FAX：(02)2735-3572
802 高雄市苓雅區新光路38號11樓之6 | TEL：(07)972-7388 | FAX：(07)972-7298