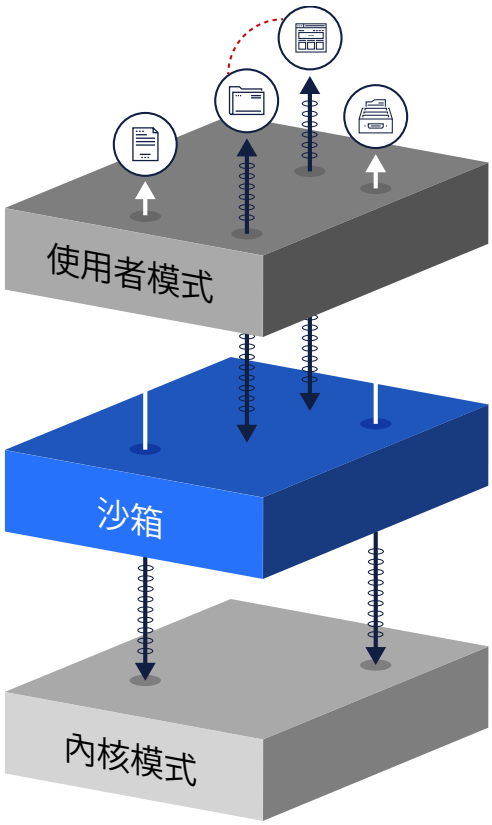
OPSWAT.

DATASHEET

OPSWAT Sandbox

為資安分析師和事件回應人員提供更智能且速度更快的 Sandbox



難以捉摸的目標性惡意軟體呈現爆炸性的成長，因此在新的惡意軟體造成危害之前，在對其做分析和分類方面的挑戰性也變得更高。此類進階的惡意軟體可以輕易躲過既有的沙盒 (Sandbox) 技術和以特徵碼為基礎的偵測工具，使企業組織面臨風險。資安團隊需要更好的偵測和分析能力，以降低攻擊的可能性和潛在影響。

OPSWAT Sandbox 在速度和準確度方面提供最新且創新的動態分析功能，並提高 IT 和運營技術 (Operational Technology, OT) 環境中的偵測率。

主要特色

無法偵測到的內核模式代理程式 (Kernel-Mode Agent)

欺騙惡意軟體執行其全部想要執行的功能，並揭露其真正的惡意性質、意圖和能耐，藉以揭示其全部的惡意性質。

超迅速且深入的掃描選項

在大約一分鐘內得出快速、而且在統計上準確的判斷，比現有當前的沙盒還要快上三倍。

深入的學習和人工智慧 (AI) 導向的分析

應用深入的學習和多重向量的偵測，方法是透過 AI 引擎來引導靜態、動態和網路輸入，以獲得更迅速且更準確的結果。

環境特定的關鍵性基礎架構防護 (Critical Infrastructure Protection, CIP) 配置文件

提供橫跨整個關鍵性基礎架構的動態分析、支援跨 IT 和 OT 環境的配置文件，例如 Windows 和特定的工業控制系統 (Industrial Control System, ICS) 平台等。

橫跨本地 (On Premise) 和私有雲端的可擴充性

支援分析資源的叢集，以將處理能力擴充至每天超過十萬個檔案。

OPSWAT.

效益

縮短分析時間

簡化在安全工程、作業和分析團隊間分析惡意軟體的流程，並加速對事件的回應，藉以縮短平均偵測時間 (Mean Time to Detect, MTTD)。

提供完整的能見度

提供單一的平台，以評估跨 IT 和 OT 環境的風險，並以獨特的方式保護關鍵性的基礎架構，使其不受目標性的零日 (Zero Day) 攻擊，尤其是在此類攻擊跨越兩個網路時。

降低分析成本

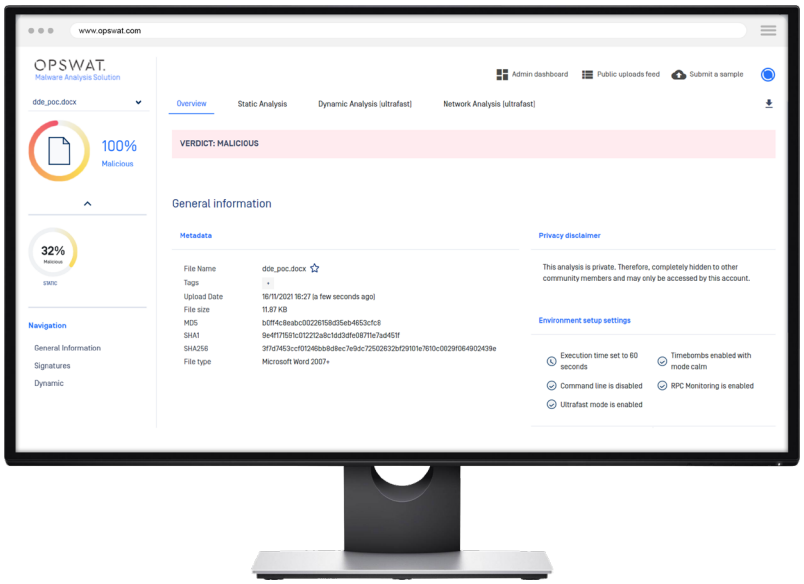
將與 IT 和 OT 有關的惡意軟體分析整合到單一的解決方案當中，藉以簡化整體的安全作業並降低成本。

提高效率和擴大規模

在大約一分鐘內執行並分析難以捉摸的惡意軟體，應用超迅速的分析和多重向量、AI 衍生的判斷，藉以支援即時的業務營運。

獲得更高的威脅能見度

透過容易解釋的分析結果 (在第三方的安全解決方案中可取得)，為資安團隊在惡意軟體行為方面提供前所未有的能見度。.



功能

應用先進的偵測功能

採取更具智慧性的惡意軟體分析方法，即保持讓攻擊者無法偵測，並如同在實時的環境中一樣記錄行為，包括指令和控制 (Command and Control, C2) 伺服器通訊等。

加速動態分析

搜尋表示有惡意軟體的關鍵異常行為，並透過 AI 傳送觀察到的結果，以迅速就 IT 和 OT 式的惡意軟體得到判斷和入侵指標 (IOC)。

提供準確的結論

從內核層級的監控中解讀大量的資料，並運用 AI 衍生的分析，以獲得更準確的結果。

支援關鍵性的基礎架構防護

支援整個關鍵性基礎架構的惡意軟體分析，針對特定的 ICS 平台和 IT 系統提供專屬的配置文件。

與 Malware Analyzer 整合

可作為 MetaDefender Malware Analyzer 的一個組成部份提供，以納入自動化惡意軟體分析的工作流程。

摘要

OPSWAT Sandbox 提供獨特的方法，以縮短惡意軟體偵測的時間，並降低與目標性攻擊有關的風險。
在傳統的動態分析解決方案運作緩慢或被老練的攻擊者躲避之際，OPSWAT Sandbox 引進獨特的創新，在無論是 IT 或 OT 基礎架構方面都可避免反偵測，並支援更大的輸出量、可擴充性以及惡意軟體的準確性，以在日常安全作業中扮演關鍵性的角色。

OPSWAT.
Trust no file. Trust no device.

For further information
https://www.opswat.com/products/metadefender/sandbox

OPSWAT.com/contact