OPSWAT.

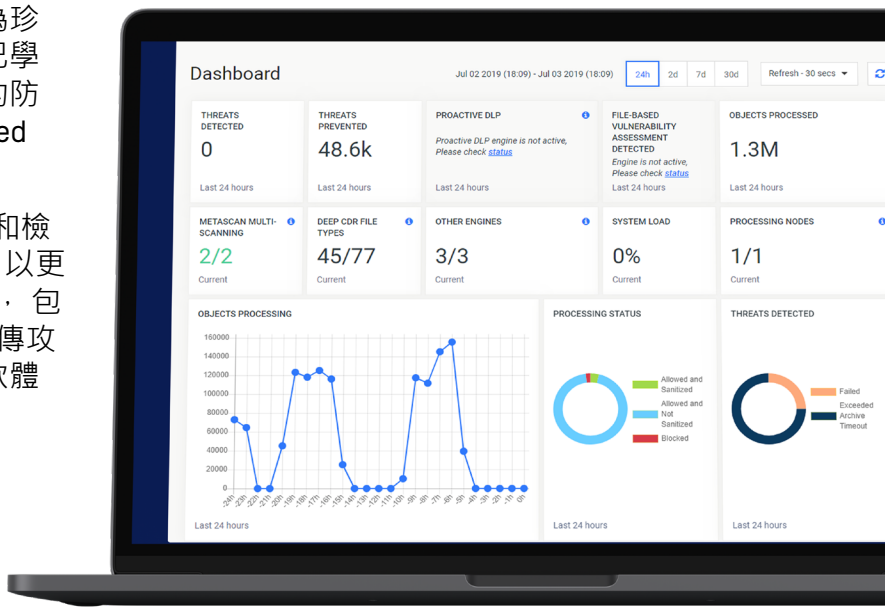
DATASHEET

MetaDefender® Core

進階威脅防護平台

您的企業不能再仰賴以檢測為主的資安系統來為珍貴資產提供妥善的保護，因為零時差惡意軟體已學會如何繞過這些防禦管道。企業需要採取更多的防範措施來對抗進階目標性攻擊 (advanced targeted attacks) 。

MetaDefender Core 讓您能將進階惡意軟體防護和檢測功能整合到既有的IT解決方案和基礎設施中，以更妥善地處理各種常見攻擊向量 (attack vectors) ， 包括：保護入口網站 (web portal) 免於惡意檔案上傳攻擊、強化資安產品，以及開發用戶本身的惡意軟體分析系統等。



效益

- 緩解關鍵系統風險並阻擋可能繞過防禦的威脅。
- 保護具辨識性的機敏個資，防止其進出組織。
- 無論是氣隙環境 (air-gapped)，或是透過 MetaDefender Cloud 使用 OPSWAT 軟體即服務方案 (SaaS) ， 都可在企業環境內的 Windows 或 Linux 伺服器上進行簡易部署。
- 支援多種程式語言，以透過 REST API 整合至企業環內。
- 藉由集中管理進行定期維護，以降低總成本。

"我們評估了沙箱、防毒和雲端多重掃描廠商，以因應零時差惡意檔案上傳的挑戰，並從中選擇了 OPSWAT 的 CDR 深度檔案清洗解決方案。"

Teza Mukkavilli
Upwork 資安長

OPSWAT.

MetaDefender Core

主要特色

深度檔案清洗(Deep CDR)
重建80多種常見檔案類型，在內容為安全的情況下，確保最大可用性，並提供數百種檔案重建選項。

多防毒引擎(Multiscanning)
整合30種以上防毒引擎中並提供彈性套裝選項。透過特徵碼、啟發式(heuristics)和機器學習等方式，主動檢測99%以上的惡意軟體威脅。

檔案為主的漏洞偵測
掃描分析二進位檔案及安裝檔，在端點裝置(包括IoT設備)執行前，檢測是否有已知的應用程式漏洞。

主動式DLP資料外洩防護
對30多種常見的檔案類型進行內容檢查，確認是否具有機敏個資［PII］，並在傳輸機敏資料前執行遮蔽或添加浮水印。

100種以上的檔案轉換選項
以實際檔案型態進行「重建」，或將檔案簡化為較不複雜的格式，維持檔案可用性及完整性。

客製化工作流程
為多防毒引擎與深層檔案清洗建立客製化工作流程，並自訂檔案處理的順序和流程。

壓縮檔掃描
多防毒引擎及深度檔案清洗可用於30多種壓縮檔。解壓縮處理選項為配置的，並支援加密歸檔。

檔案類型辨識
可辨識超過4,500種檔案類型，並依據檔案內容確認實際檔案類型，而非用可信度低的副檔名來防禦檔案欺騙攻擊。

OPSWAT 保護關鍵基礎設施，並以消除惡意軟體和零時差攻擊為首要目標。 OPSWAT 相信，每個檔案和每個設備都可能是潛在威脅，必須隨時在所有位置應對威脅（包括進入、退出和靜態狀態）。因此，OPSWAT 的產品專注在威脅防護及流程建立，以實現安全的資料傳輸和設備存取，進而讓生產系統的資安風險降到最低。這也就是為什麼美國98%的核電單位都信任 OPSWAT 所提供的網路安全性與合規性。

進一步了解 MetaDefender Core 相關資訊，請參閱 OPSWAT.com/products/metadefender/api

聯絡 OPSWAT 技術人員，請參閱 OPSWAT.com/contact

OPSWAT.
Trust no file. Trust no device.