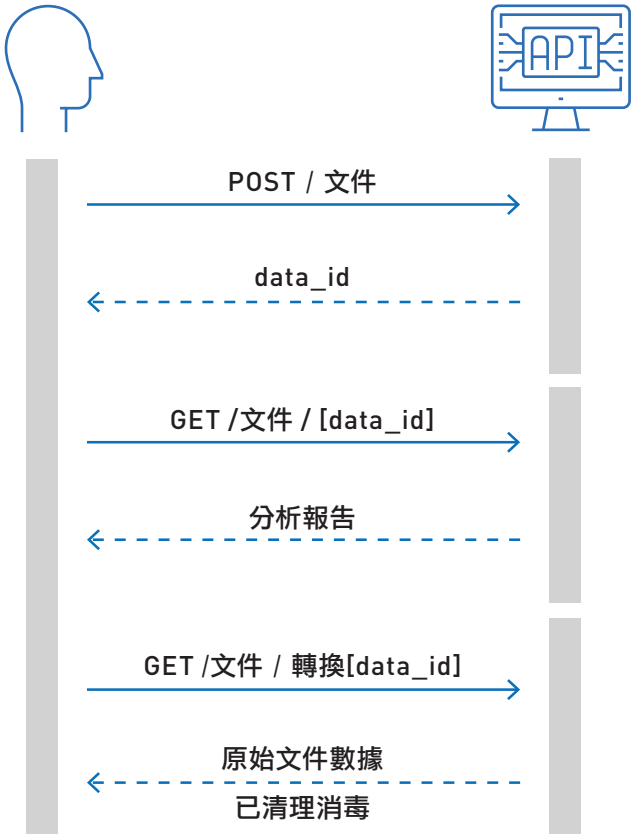
OPSWAT.

MetaDefender® API
進階威脅防禦開發平台

MetaDefender API允許您將進階惡意軟體防護和偵測整合到您的IT解決方案及應用程式中。MetaDefender提供領先業界的多重掃描、數據清理消毒以及漏洞掃描，以防止已知和未知的威脅，包括勒索軟體與零時差攻擊(zero-day attacks)。使用我們的REST API，您可以很容易地整合數據清理消毒和30多種反惡意軟體引擎到您的既有系統中，以針對網路安全威脅進行檢測和預防。此外，我們龐大且不斷增長的漏洞數據庫允許您查找位於安裝程序、二進制文件和物聯網(IoT)韌體中的漏洞。

獨立軟體供應商[ISV]和惡意軟體研究人員使用MetaDefender API來強化其現有解決方案，IT管理員可為系統添加進階威脅防護以提供惡意文件上傳防護功能。



效益

多重掃描—以運用特徵碼、啟發式和機器學習技術的超過30種反惡意軟體引擎進行掃描，藉以最快和最早地檢測已知和未知的威脅。

檔案清洗消毒[CDR]—解構超過70種常見檔案格式，並重建每個文件，確保安全內容的完整可用性。

漏洞掃描—使用超過10億個雜湊值(Hash)檢測超過15,000個軟體應用程式中的已知漏洞。

「我們針對零時差攻擊惡意軟體文件上傳挑戰，評估了沙盒(sandboxes)、AVvendors和雲端多重掃描供應商，而(最終)選擇了OPSWAT的數據清理消毒。」

Upwork安全負責人
Teza Mukkavilli

MetaDefender API功能

檔案清洗消毒[CDR]—解構超過70種常見文件類型，並重建每個文件，確保安全內容的完全可用性。

多重掃描—提供超過30種領先的反惡意軟體引擎，可以彈性的選購不同軟體包；本軟體模組包含第三方反惡意軟體原廠合法授權，客戶無須自行添購防毒軟體授權。

漏洞掃描—掃描二進制文件和安裝程序，以便在端點設備（包括IoT設備）上執行之前檢測已知的應用程式漏洞。

壓縮檔處理—透過改善的高速解壓引擎，將檔案由壓縮檔中提取，以偵測惡意程式並避免壓縮檔炸彈攻擊。

文件類型驗證—驗證超過4500種文件類型，以對抗文檔格式竄改攻擊。

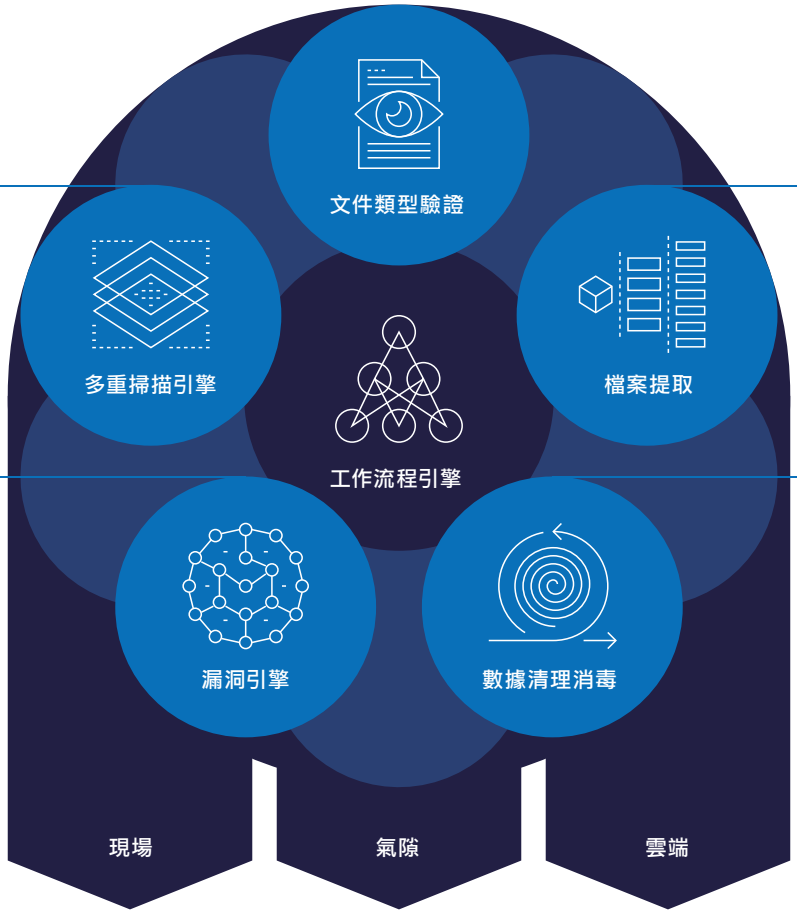
REST API—使用幾乎任何的編程語言來整合Meta Defender技術。

100多個文件轉換選項—透過文件類型的真正「重建」、或將文件展平為較為簡單的格式，保持文件的可用性和完整性。

工作流程引擎—為多重掃描和檔案清洗消毒[CDR]創建自己的工作流程，並且自定義處理文件的順序和流程。

部署平台—在您的[作業]環境中的Windows或Linux伺服器上進行部署，亦支援實體隔離網路部署以及更新。或者也可以在我們的雲使用metadefender.com 雲端服務。

MetaDefender架構



30+
反惡意軟體

AhnLab, Symantec, nProtect, Kaspersky, McAfee, F-Prot, ESET, Bitdefender, AVG, LavaSoft, Zillya, Total Defense, Sophos, Quick Heal, Cyren, Trend Micro, Ikarus, Avira

30+
支援的檔案

AR, ARJ, CAB, CHM, CPIO, CRAMPS, DMC, EXT, FAT, CPT, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, UDF, UEFI, VDI, VHD, and more...

15,000+
支援的應用程式

Adobe, Excel, Java, Powerpoint, Skype, Word

30+
支援的檔案類型

DOC, DOCX, HTML, JPG, PDF, PPT, PPTX, XLS

OPSWAT.
Trust no file. Trust no device.

橙鋐科技 ORANGERED

業務洽詢

周建全 Dunken Chou
0936961166
dunken@ortech.com.tw

邱瓊瑤 Joanne Chiou
0937519941
joann.chiou@ortech.com.tw

www.opswat.com