

# OPSWAT.

## 安全數據交換流程

### 保護關鍵網路免受網際威脅侵害

包括關鍵基礎設施、政府機構部門和金融機構等需要最高安全級別之組織，使用 MetaDefender 以實現將文件攜入和攜出組織的安全方式，並防止網際網路安全威脅。

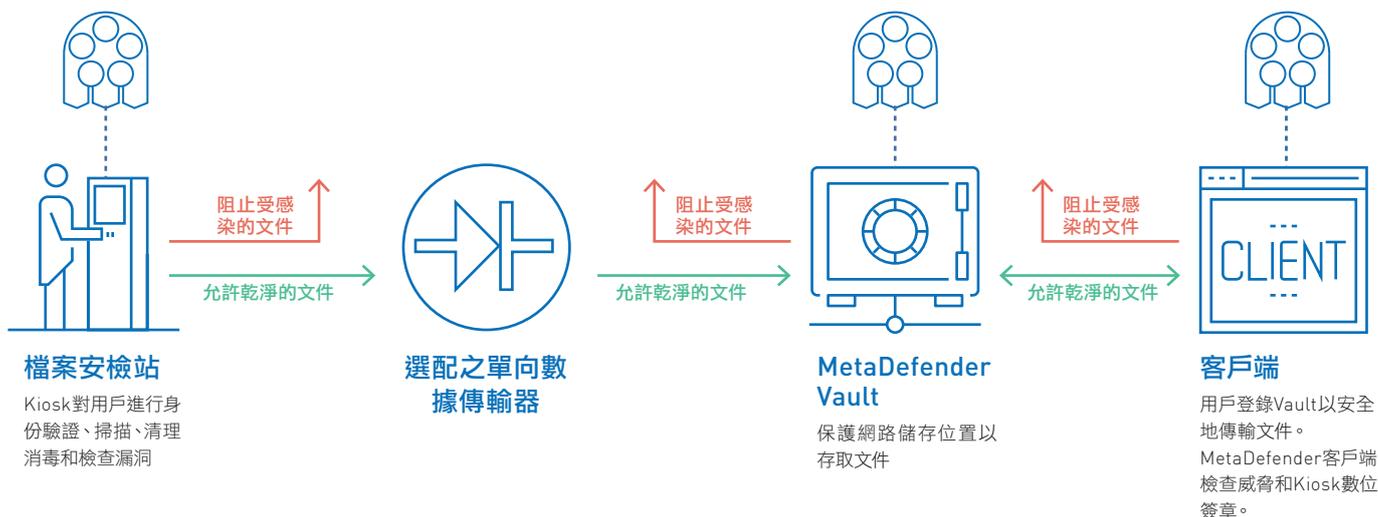
由於嚴格的系統停機時間要求、法規，以及透過可攜式設備和USB磁碟機以及手機等媒體引入惡意軟體的風險，維運隔離網路或實體隔離網路（air-gap network）相當具有挑戰性。2015年，對烏克蘭電網的襲擊導致70萬人無電可用。關鍵基礎設施如何確保惡意文件在允許使用可攜式媒體設備的同時不受影響呢？

MetaDefender使您能夠創建安全的端到端流程，以便將文件由關鍵網路傳輸出入。

- 防禦透過USB和其他可攜式設備以及SD卡、CD / DVD和手機等媒體引入的攻擊。
- 根據用戶和角色為文件類型和安全性處理創建精細的安全策略。
- 啟用文件傳輸的可見性和審核。
- 使用多重掃描(multi-scanning)、檔案清洗消毒（CDR）以及漏洞檢測來預防已知以及未知之威脅。



### 保全文件傳輸



# MetaDefender Kiosk

## 可攜式媒體檢查站

MetaDefender Kiosk 是一個檢查站，用於在安全威脅進入隔離網路之前檢測且阻止它們。 Kiosk可以部署在整個組織的戰略位置、員工或訪客可能會使用可能夾帶惡意檔案的USB磁碟或其他可攜式媒體。

MetaDefender Kiosk 可以利用 MetaDefender 的任何核心防禦技術，另外還包括產品特定功能如：本地化、可客製的用戶界面[UI]、單向數據傳輸器整合、數位簽章結合文件有效驗證檔案雜湊避免竄改 (file hash verification) 等。 MetaDefender Kiosk 被絕大多數美國核能電廠採用，使 MetaDefender 成為美國核子工業領先的、以硬體為主的可攜式媒體檢測暨文件清理消毒解決方案。

### 重要功能

- 可客製化的多語言用戶界面
- 與MetaDefender Vault無縫整合
- 防止可攜式設備和媒體(包括：USB驅動器、SD卡、CD / DVD和手機)中的威脅
- 可以對允許的文件和媒體進行數位簽名
- 能夠阻止或隔離惡意文件
- 支援加密媒體設備和設備白名單
- 支援依據用戶或角色的可配置工作流程

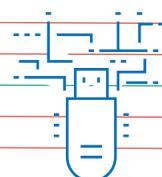
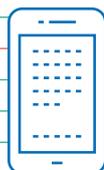
# MetaDefender 客戶端

## 端點的額外威脅防護

MetaDefender 客戶端可保護組織中的端點免受以USB為基礎的威脅，可以使用 MetaDefender 領先業界的威脅防禦技術，掃描和消毒可攜式媒體，補充現有的防毒和端點保護。MetaDefender 客戶端還可以驗證 MetaDefender Kiosk 已簽署的數位簽章，如此可以節省時間並確保端點只能使用獲得周邊Kiosk掃描檢查並簽署的文件。

### 重要功能

- 保護端點免受以可攜式媒體和設備為主的攻擊
- 除非已符合安全政策，否則阻止存取USB磁碟和其他可攜式媒體設備
- 支援 MetaDefender Kiosk 應用的數位簽章驗證
- 透過使用多個反惡意軟體引擎掃描系統，提供第二層防禦應付威脅



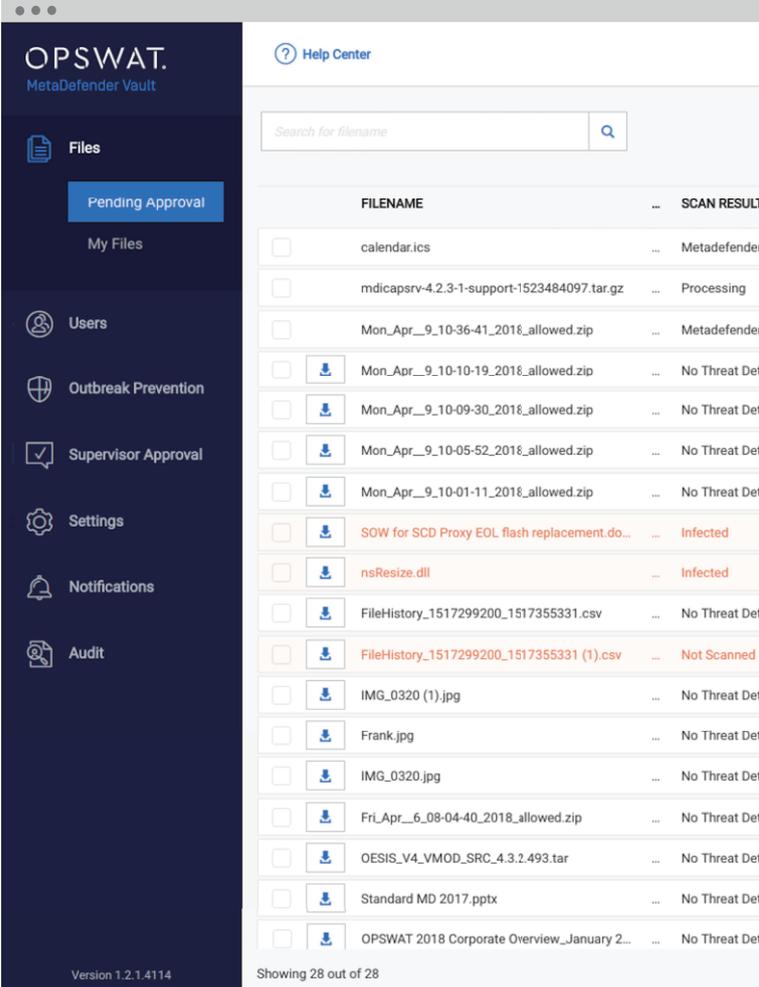
# MetaDefender Vault

## 保全文件傳輸和儲存

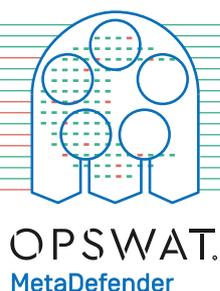
MetaDefender Vault 是一個受保護的網路儲存位置，可以部署於網路上的任何位置，無需任何硬體，並且可以與 MetaDefender Kiosk 整合用於儲存已檢查和處理的文件。該解決方案可以將安全文件傳入和傳出隔離之網路，而無需將可攜式媒體傳輸到組織中。訪客或用戶可以從 MetaDefender Vault 存取所有經過認證和檢查的文件，同時將所有USB磁碟留在外圍。可以戰略性地建立隔離網路中的檢查點，以便在必要時進行可見性、審查和惡意軟體防護。

### 重要功能

- 易於安裝並與 MetaDefender Kiosk 和客戶端整合
- 可以使用瀏覽器傳輸文件，因此不需要特殊的客戶端軟體
- 可以將文件隔離檢疫，在留存特定時段後才允許下載，以防止惡意程式檢查的空窗期
- 管理員角色和細部日誌（granular logging），以提高可審查性
- 主管批准流程將人因考量於系統中，在解鎖上傳文件之前查看掃描結果並進行審核



	FILENAME	SCAN RESULT
<input type="checkbox"/>	calendar.ics	Metadefender
<input type="checkbox"/>	mdicapsrv-4.2.3-1-support-1523484097.tar.gz	Processing
<input type="checkbox"/>	Mon_Apr_9_10-36-41_2018_allowed.zip	Metadefender
<input type="checkbox"/>	Mon_Apr_9_10-10-19_2018_allowed.zip	No Threat Det
<input type="checkbox"/>	Mon_Apr_9_10-09-30_2018_allowed.zip	No Threat Det
<input type="checkbox"/>	Mon_Apr_9_10-05-52_2018_allowed.zip	No Threat Det
<input type="checkbox"/>	Mon_Apr_9_10-01-11_2018_allowed.zip	No Threat Det
<input type="checkbox"/>	SOW for SCD Proxy EOL flash replacement.do...	Infected
<input type="checkbox"/>	nsResize.dll	Infected
<input type="checkbox"/>	FileHistory_1517299200_1517355331.csv	No Threat Det
<input type="checkbox"/>	FileHistory_1517299200_1517355331 (1).csv	Not Scanned
<input type="checkbox"/>	IMG_0320 (1).jpg	No Threat Det
<input type="checkbox"/>	Frank.jpg	No Threat Det
<input type="checkbox"/>	IMG_0320.jpg	No Threat Det
<input type="checkbox"/>	Fri_Apr_6_08-04-40_2018_allowed.zip	No Threat Det
<input type="checkbox"/>	OESIS_V4_VMOD_SRC_4.3.2.493.tar	No Threat Det
<input type="checkbox"/>	Standard MD 2017.pptx	No Threat Det
<input type="checkbox"/>	OPSWAT 2018 Corporate Overview_January 2...	No Threat Det



# MetaDefender 的優勢

**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。

**數據清理消毒[CDR]**—解構70多種常見文件類型，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 Value）檢測超過15,000個軟體應用程式中的已知漏洞。

**文件處理選項**—阻止、隔離或數位簽名和驗證文件。

**文件類型驗證**—能夠驗證文件類型並僅允許複製獲批准的文件類型。

# MetaDefender 架構

