OPSWAT.

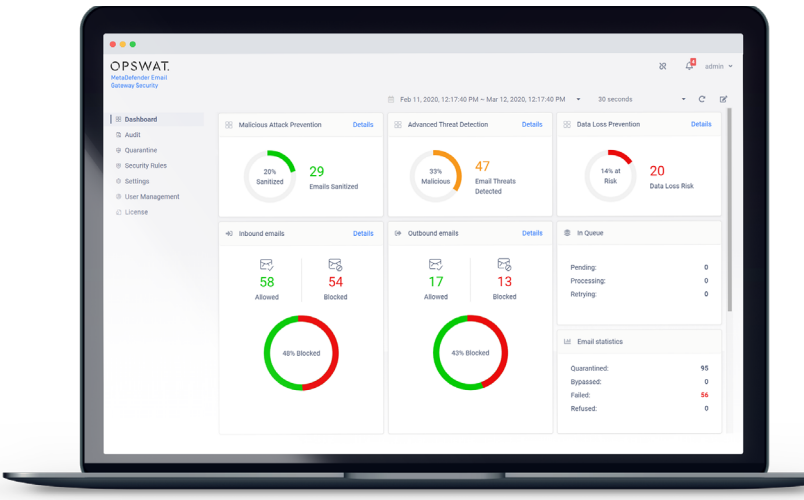
DATASHEET

MetaDefender® Email Gateway Security

提供信件匣所需的可信度

大部分的惡意軟體都是透過電子郵件啟動的。看似安全的連結和附件可能包含惡意內容，一旦被存取，惡意軟體就會在網路中複製、散佈。

MetaDefender Email Gateway Security 在傳送前會檢查每封電子郵件和附件、掃描惡意內容、重建可疑附件並刪除敏感資料。



掃描 · 修復 · 傳送

進階威脅可以繞過目前電子郵件安全解決方案所使用的惡意軟體檢測應用程式。對抗來自電子郵件惡意軟體的三種最佳方式：

1. 盡可能使用多種掃毒軟體
2. 拆解並重建附件以阻擋威脅
3. 檢查連結的惡意行為並加以移除

MetaDefender Email Gateway Security 能在不影響員工工作的情況下，為舊版電子郵件閘道提供加值防護，移除99%以上隱藏在電子郵件內的惡意軟體。

MetaDefender Email Gateway Security 可讓您安心無虞，沒有資安疑慮。

效益

零時差惡意軟體防護
移除未知內容並輸出乾淨、可用的檔案

進階威脅防護
使用30種以上的防毒引擎進行電子郵件掃毒

主動阻擋網路釣魚
將指向不安全URL的超連結替換為純文字，或重新導向信譽檢查，以防止用戶不當操作

避免機敏資料外洩
檢測、編輯或阻擋機敏資料的接收、發送

整體檢查及修復
整封電子郵件都會被檢查：包括標題、內文和附件

移除受密碼保護的附件
這是處理加密附件最簡便的解決方式

安全儲存附件以防止病毒擴散
自動將附件上傳到用戶的安全儲存空間內，以進行核准並防止病毒大幅擴散。

OPSWAT.

MetaDefender Email Gateway Security

主要特色

防止惡意電子郵件
能清洗85種以上常見檔案類型並重建每個附件，以確保內容安全性和最大可用性。

惡意軟體檢測
每封電子郵件都由30種以上防毒引擎加以分析，並透過特徵碼、啟發式[heuristics]和機器學習等技術來辨識各種已知和未知威脅。

檢查郵件是否有機敏個資[PII]
在郵件內容離開或進入組織前，檢查電子郵件標題、內文及附件是否具有機敏資料。

安全儲存附件
所有附件都會傳送到獨立的儲存空間，以持續進行掃毒及病毒阻擋，且檔案會在主管核准後才放行。

動態阻擋網路釣魚
為了找出潛在的網路釣魚攻擊，嵌入的超連結將被替換為純文字URL，或重新導向信譽檢查。

電子郵件處理流程

用戶收到的附件都是經過掃描和修復過的內容，因此不會有任何惡意檔案傳到內部。OPSWAT 為企業的電子郵件處理流程提供第二道安全防線。

- 傳輸代理 – 當 Microsoft Exchange Server 可用時，電子郵件將透過傳輸代理傳送。
- **SMTP** – 在其他電子郵件閘道（非 Exchange）可用的情況下，郵件則透過SMTP傳送。
- **x-Headers** – 用於 MetaDefender Email Gateway Security 與郵件伺服器之間的溝通。

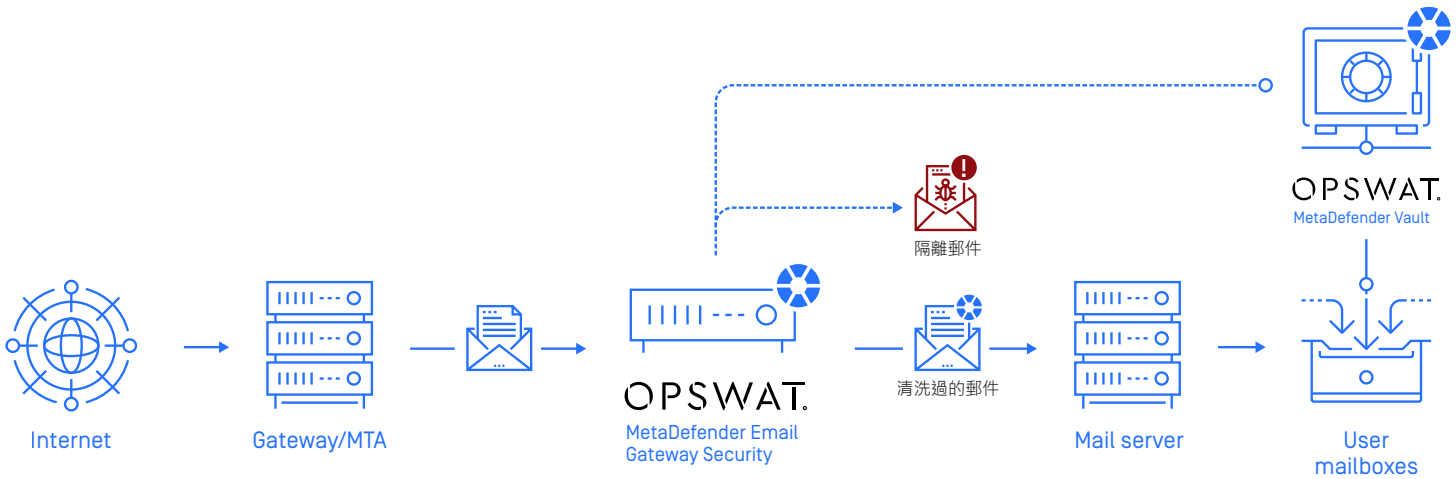
技術規格

支援作業系統
Microsoft Windows, 64 位元

最小硬體需求
- **CPU: Intel Core i5-8500 處理器、 內建六核心**
- **RAM: 32 GB DDR4**
- **SSD: 256 GB**
- **NIC: 1GbE**

整合方式
- **SMTP**
- **Exchange transport agent**
- **x-Headers**

效能
最高每小時10,000封電子郵件



為了進行評估，MetaDefender Email Gateway Security 提供了三種可用選項：**旁聽監控**、**Inline監控**，以及**透過SPAN port進行部署**。

OPSWAT.
Trust no file. Trust no device.