OPSWAT.

DATASHEET

MetaDefender®
電子郵件防護閘道

提升您的電子郵件安全防護能力

電子郵件仍然是主要的攻擊途徑。企業組織面臨越來越複雜的社交工程手段，誘使使用者執行惡意程式碼，利用未知的應用程式漏洞，導致網絡遭受入侵。而對於零時差威脅的防護常常緩慢且無效率，更進一步加劇了這些問題帶來的挑戰。

OPSWAT MetaDefender電子郵件防護閘道引入了一些重要功能，將電子郵件保護提升到更高效的水準，以實現先進的安全防護政策。

主要特点

防釣魚和防垃圾郵件:

我們的解決方案採用先進的多階段防釣魚技術，以避免人為錯誤。 通過結合多種檢測技術，電子郵件通過一系列黑名單和內容過濾技術，識別垃圾郵件、社交工程、勒索欺詐和惡意釣魚攻擊。

零時差惡意軟體防護:

Deep CDR是一種先進的威脅防護技術，能夠通過消毒超過120種文件類型和電子郵件中的惡意活動內容，使組織能夠保護自己免受未公開的零時差威脅的攻擊。我們的方法比基於偵測的安全性快30倍。

管理有密碼保護的附件:

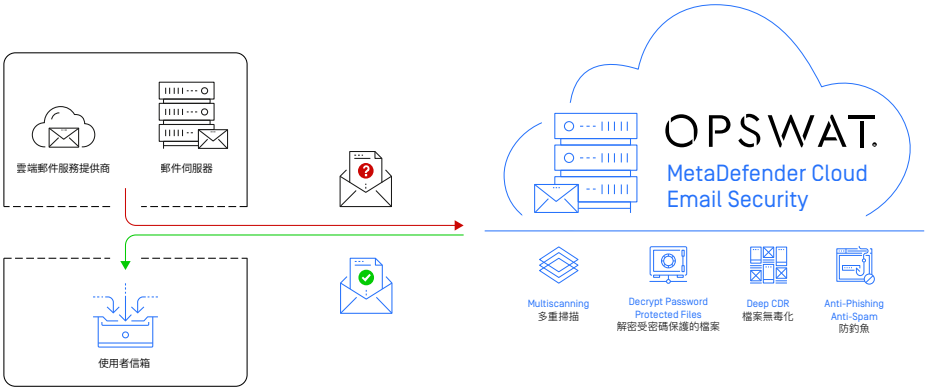
對於有密碼保護的附件，需要提供解密密碼，以應用Deep CDR和Multiscanning。

進階威脅防護:

多引擎掃描技術提高了對惡意軟體和進階威脅的偵測率，同時將漏洞偵測時間減少到幾乎為零。除了傳統的簽名偵測外，多引擎掃描技術利用啟發式和機器學習引擎來應對未知威脅。

OPSWAT.

MetaDefender Cloud Email Security



性能

增強對高級威脅的檢測
Multiscanning技術使用多達35個防惡意軟體引擎，通過特徵、啟發式和機器學習技術對每封電子郵件進行分析。

減少漏洞暴露時間

Multiscanning技術結合了多個防病毒引擎的更新來源，減少了企業的漏洞暴露時間。MetaDefender Core的套裝組合可以顯著降低暴露時間，使其少於7分鐘。

預防零時差攻擊
通過刪除潛在惡意內容來保護每封電子郵件的內容和附件。只有透過檢測並重組、完全可用的文件允許進行傳送。我們的解決方案對包括受密碼保護的附件在內的120多種常見文件類型進行了消毒。

利用動態反釣魚技術
動態反釣魚技術針對多個階段的釣魚攻擊進行處理。它應用先進的啟發式、神經網絡和魚叉式釣魚過濾器，以及IP/發件人和內容信譽進行檢查，以防止釣魚攻擊。

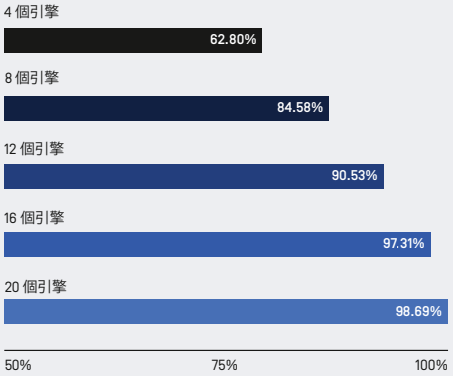
保護個人身份信息和敏感數據遺失
主動數據丟失預防(DLP)有助於符合PCI、HIPAA、GLBA、GDPR和FINRA等行業法規，並防止敏感內容意外進入或離開企業組織。它可以自動遮蔽40多種文件類型，包括PDF和Office文件。對於圖像，它採用影像辨識(OCR)技術。

*=根據部署選項而定

效益

- 透過在多個階段發現潛在的釣魚攻擊，減少人為錯誤
- 保護用戶免受社交工程攻擊，確保 IT 部門能夠減低人員行為造成的負擔
- 確保符合 PCI 和其他郵件相關的法規，並保護公司內部的個人身份信息(PII)數據
- 提高惡意軟體檢測的效果，以提供先進的郵件保護層級
- 減少對惡意軟體的漏洞期(WoV)，有效防止惡意軟體爆發
- 通過從附件中移除基於文件的威脅，保護業務生產力文件
- 依靠預防而非檢測，有效消除零時差針對式攻擊的威脅

OPSWAT多引擎掃描技術對於前10,000個威脅的檢測率



總結

OPSWAT MetaDefender電子郵件閘道安全引入了一些關鍵功能，填補了安全漏洞，降低了郵件的網路安全風險，並消除了潛在的人為錯誤，提升郵件安全至更高的水平。通過應用OPSWAT技術，我們的解決方案使組織能夠更好地保護自己免受複雜攻擊的影響，包括當今常見的未公開和零時差威脅。我們的解決方案可作為雲端服務和本地部署兩種方式提供。

聯絡我們