醫療業贖金軟體攻擊增加50%！全球第二大醫療保健提供商採用OPSWAT技術保護其關鍵網路

根據 CyberThreat Intelligence Integration Center 的報告，自 2022 年以來，全球針對醫療照護企業的贖金軟體攻擊幾乎增加了一倍。為何在醫療照護領域會有如此大的升幅?

根據美國衛生與人類服務部最近針對醫院復原狀況所做的研究，醫療照護設施對網際網路連線系統的依賴、大量敏感的個人識別資訊和個人健康資訊資料，以及設施對營運連續性的重要需求，是這個領域成為首要攻擊目標的三大主要原因。

身為全球第二大、以色列最大的健康維護組織 (HMO)，Clalit Health Services 透過 1,600 多間診所和 14 間醫院，為超過 52% 的以色列人口提供醫療服務。自 2023 年以來，針對 Clalit 的資安威脅急遽增加，因此 Clalit 成為頻繁的網路攻擊目標也就不足為奇了。正如 Clalit 安全與基礎建設通訊主管 Zahi Ben-Abu 所解釋的，「作為以色列醫療保健領域的重要基礎建設，我們之前的解決方案並未達到我們的安全標準」。

為了符合其內部的高標準，並遵守政府對以色列醫療保健提供者的嚴格規定，Clalit 向 OPSWAT 的專家求助，希望能建立一套完整的解決方案，以確保其關鍵基礎架構受到完整的保護。

每日面臨大量資料的檔案安全挑戰

Clalit 每天要處理約 500 萬個來自不同來源和檔案類型的檔案，其中許多都包含敏感的病患健康資訊。因此，最重要的是需要一套解決方案，能夠處理如此龐大的數量、提供擴充性與彈性，並確保所共用的檔案不含惡意軟體。

「作為以色列醫療保健領域的關鍵基礎設施，我們之前的解決方案不符合我們的安全標準。」

Zahi Ben-Abu——安全與基礎設施通訊主管

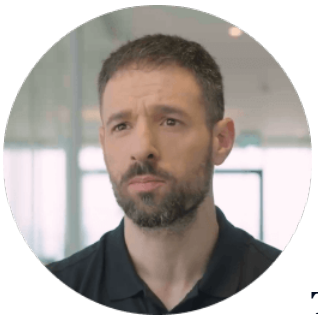
在 Clalit，檔案可能來自許多來源，包括合作公司、供應商、醫院、銀行、法律組織和政府機構。這些檔案也有許多形式，包括 CSV、PDF、Word、醫療影像和二進位檔案，因此解決方案也需要能夠處理各式各樣的檔案類型。

最重要的是，Clalit 需要一種方法來保護他們的基礎架構，防止惡意檔案從任何外部來源進入他們的系統。

創造保護基礎設施的新模式

Clalit 安全與基礎建設通訊主管 Zahi Ben-Abu 解釋：「我們看到為所有檔案掃描機制建立集中化管理解決方案的價值。」

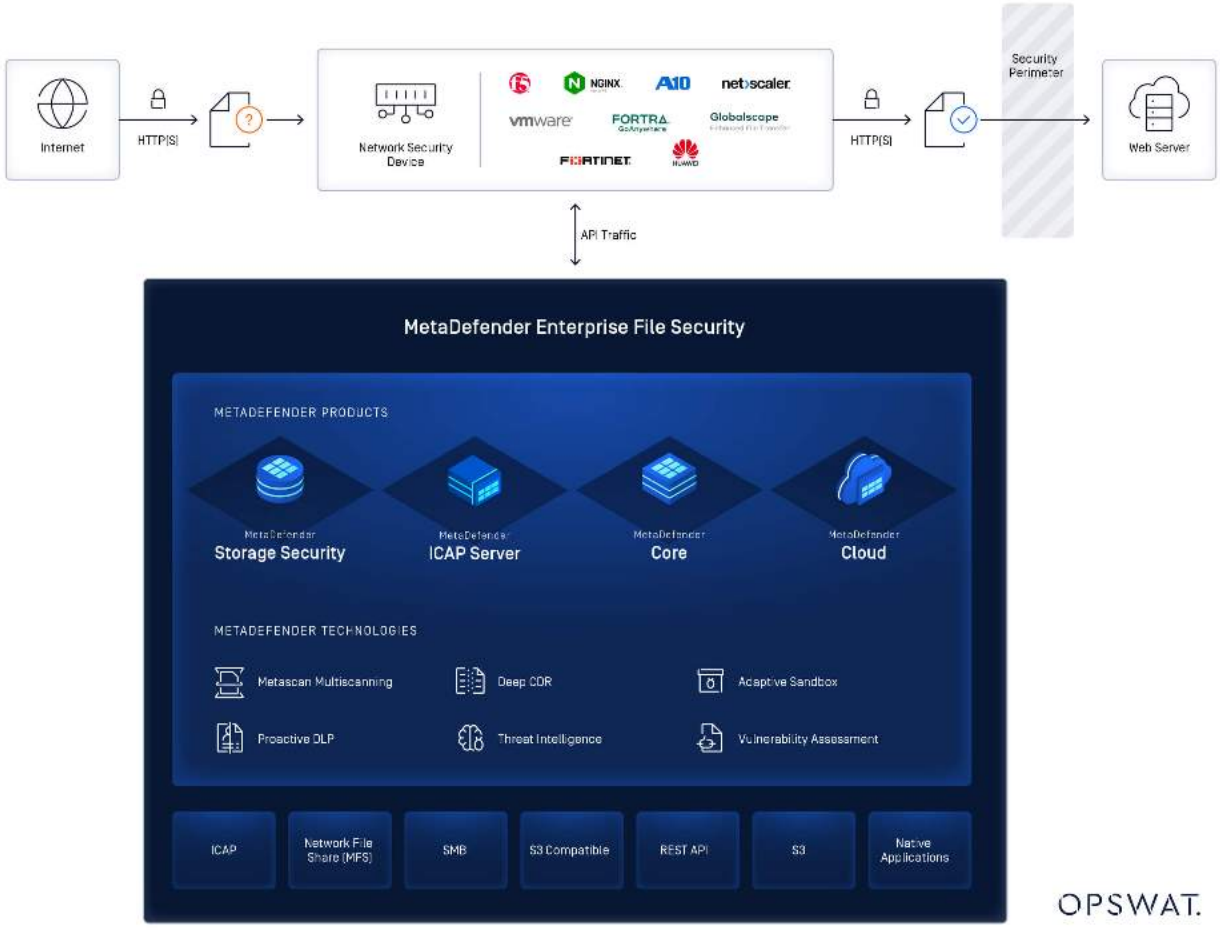
「我們首先透過API 整合Managed File Transfer (MFT) 和電子郵件安全解決方案。接著我們將ICAP 伺服器連接到我們的反向代理和API 閘道，以提供掃描檔案上傳和網路應用程式流量的能力。」



Tamir Shahar——網路架構設計師

目前，所有透過電子郵件、API 、管理式檔案傳輸、網際網路和雲端等管道進入 Clalit 的檔案，都會經過 13 個防毒引擎和Deep CDR 技術的掃描。如果檔案無法通過 CDR 或被排除在外，則會被傳送到 MetaDefender Sandbox作進一步分析。所有掃描都是透過API 或 ICAP 線上進行。

正如 Clalit 的關鍵基礎建設與網路主管 Omer Keidar 所描述的：「有了OPSWAT ，我們的資料安全有了保證，我們的檔案沒有惡意軟體」。



OPSWAT的保護層內幕：我們的技術如何保護 Clalit 的基礎設施

透過假設每個檔案都包含潛在威脅，例如惡意軟體或零時差漏洞，檔案無毒化CDR (Content Disarm and Reconstruction) 會重新產生安全、可用的檔案，解除威脅。Deep CDR 技術以「預防」為主的防禦方式，強化以偵測為基礎的反惡意軟體掃描，保護組織免受以檔案為基礎的威脅，包括有針對性的攻擊。

OPSWAT的Deep CDR 透過消除威脅並重建檔案來清理檔案，以防止基於檔案的漏洞。傳統的安全措施並不總是能偵測到複雜的網路威脅，包括零時差攻擊。Deep CDR 針對這一點，在細微的層級上對檔案進行淨化，從而降低先進和新興威脅的風險。

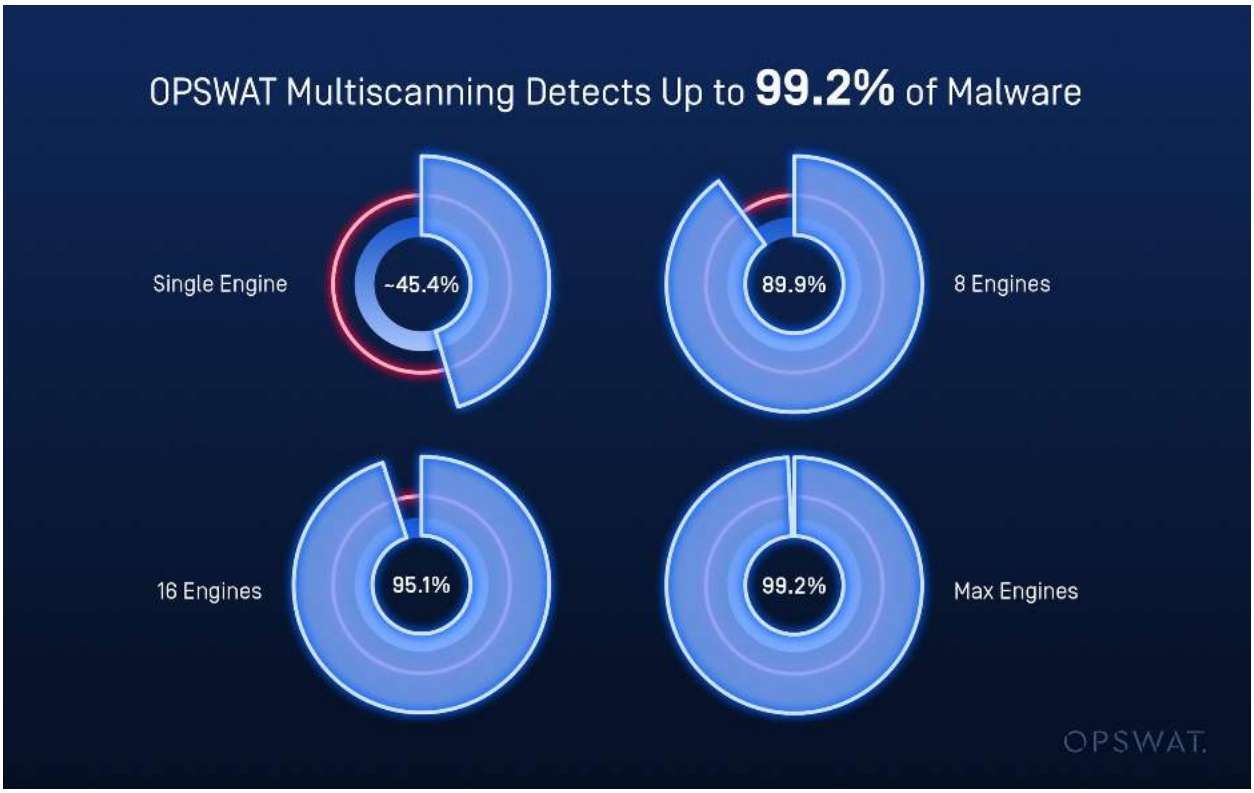
Clalit 網路安全的關鍵部分仰賴OPSWAT的獨特多防毒引擎（Multiscanning）技術，該技術提供先進的威脅防護，與單一供應商的反惡意軟體解決方案相比，可提高偵測率、縮短疫情偵測時間，並提高偵測精確度。

透過共同合作和擴充 Deep CDR、Multiscanning 等技術，可提供重要的防護層，以對抗通常以醫療保健提供者為目標的進階及零時差威脅。

研究顯示，當部署的反惡意軟體引擎越多，惡意軟體的偵測率就會越高。在OPSWAT的解決方案中，每個引擎的優點結合起來，提供卓越的偵測能力，以更快的速度識別出更多

的威脅。透過結合多個掃描引擎的結果，OPSWAT 可以縮短曝露時間，提供威脅的全球可見性，並達到惡意檔案幾乎零曝露。

在最近針對 10,000 多個最活躍威脅進行的多重掃描測試中，OPSWAT 使用 12 個聯合引擎的偵測率超過 90%，使用 16 個引擎的偵測率超過 95%，使用 20 個或更多引擎的偵測率超過 99%。

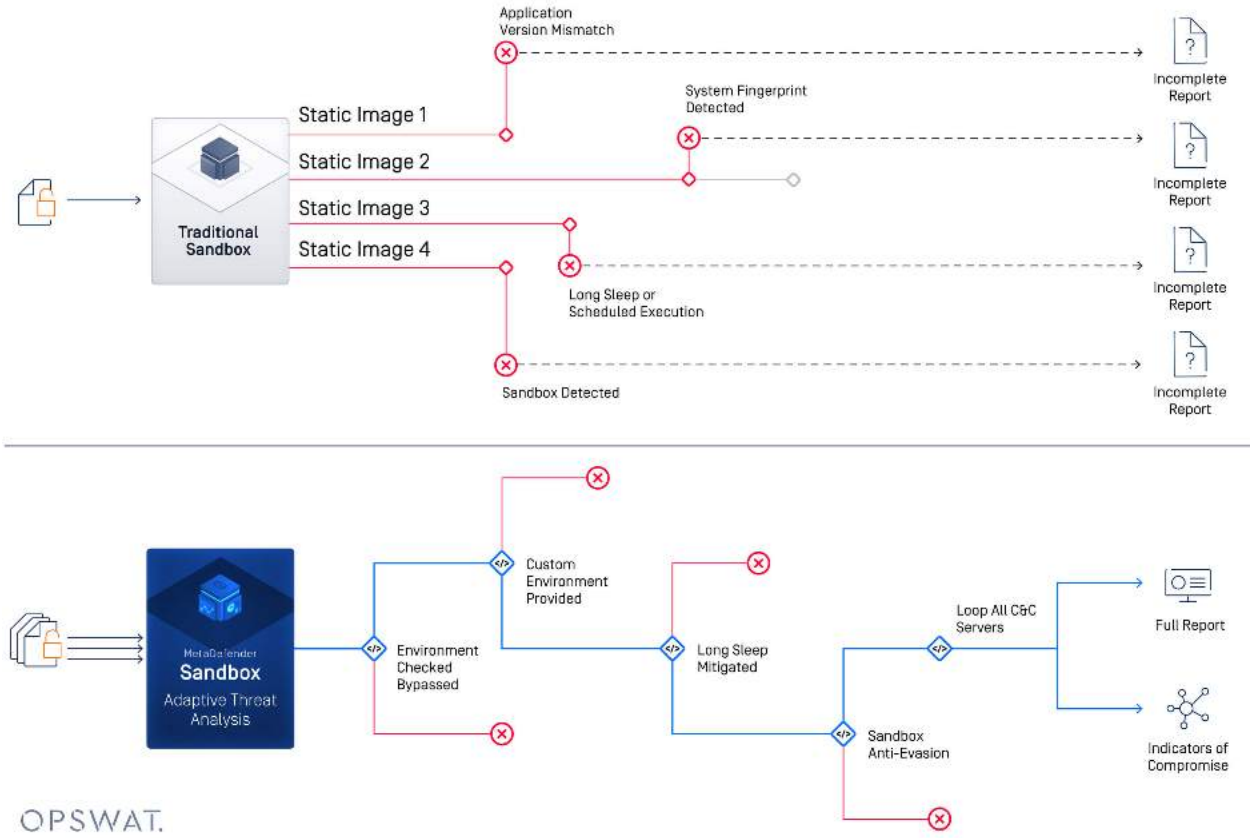


隨著檔案數量的增加，以及威脅份子不斷改良其技術，創造出愈來愈複雜的惡意軟體來躲避安全解決方案，組織需要能夠快速掃描大量檔案、找出惡意軟體，並同時擊敗每一層混淆，以辨識有價值的 IOC (入侵指標)的掃描技術，並且符合低資源需求、易維護且高效率的能力。

延伸閱讀：多防毒引擎掃描的優勢在哪裡?

MetaDefender Sandbox其獨特的自適應威脅分析技術擷取 IOC 的速度，比傳統沙箱快 10 倍，同時吞吐量也高出 100 倍。僅在一台伺服器上，MetaDefender Sandbox 就能每天處

理 25,000 個或更多檔案，其自適應威脅分析技術可在擷取更多 IOC 的同時，進行零時差惡意軟體偵測。



「OPSWAT Sandbox 具備非常快速的判定速度，這要歸功於模擬功能，並與其他產品如 Deep CDR整合。因此，在掃描檔案時可提供最佳的線上體驗，對使用者的干擾降至最低，並可進行簡易管理。」

Tamir Shahar——網路架構設計師

OPSWAT的解決方案相互配合，可確保 Clalit 的關鍵基礎設施受到全面保護。

以更好的解決方案創造價值

Clalit 的技術團隊很快就指出，透過OPSWAT 解決方案，有許多好處讓他們更容易保護關鍵基礎設施免受威脅。

「OPSWAT的Deep CDR 支援最廣泛的檔案格式，包括文檔、影像和多媒體檔案，」Clalit 的基礎架構設計師 Tamir Shahar 表示。

「此外，Deep CDR 可在解除後，以高保真方式重建檔案。這表示已清除的檔案仍保留原始格式和功能，將對可用性和生產力的影響降至最低。這與其他 CDR 解決方案形成強烈對比，因為其他 CDR 解決方案可能會在清除過程中刪除過多內容或功能。」

Clalit 的網路專家指出，使用OPSWAT 的其他優點包括：

- **強化使用者體驗**：沙箱透過模擬功能可快速產生判決，並可輕鬆與Deep CDR 等其他產品整合。這可在掃描檔案時提供最佳的線上體驗，並將對使用者造成的干擾降至最低。
- **節省時間**： OPSWAT的沙箱對於偵測未知威脅至關重要，它模擬檔案的速度比一般沙箱快 10 倍。
- **優異的檔案支援**：多種防毒引擎提供 Clalit 彈性，可支援所有檔案、類型及不同情況，例如無法消毒的檔案。

「透過OPSWAT ，我們可以確保資料安全，檔案不含惡意軟體。」

Omer Keidar——關鍵基礎設施與資安技術主管

提供全面保護

由於他們每天處理的數百萬個敏感檔案，Clalit 需要一個以最創新的技術為後盾的全面保護計劃。OPSWAT是同級產品中最佳的解決方案，並透過不斷創新來滿足瞬息萬變的威脅環境，Clalit 現在已成為醫療照護組織保護其關鍵基礎架構的典範，同時讓客戶放心其敏感的醫療照護檔案受到徹底保護。

正如 Zahi Ben-Abu 所總結的，「有了OPSWAT ，我們有信心確保客戶敏感資料和資訊的安全」。

您的關鍵基礎設施也面臨資安威脅嗎？ 預約OPSWAT專家諮詢最適合您的解決方案