使用安全且易於管理的檔案傳輸系統保護關鍵能源基礎設施

（由於業務性質特殊，為保護其業務內容，本客戶案例的組織名稱以EnergyCo代稱。）

根據一份 關鍵基礎設施網路攻擊報告 顯示，能源組織是網路威脅者的重點攻擊對象，被攻擊的比例達到了驚人的 39%，是第二大最常被攻擊的產業——關鍵製造業（11%）和運輸行業（10%）的三倍之多。

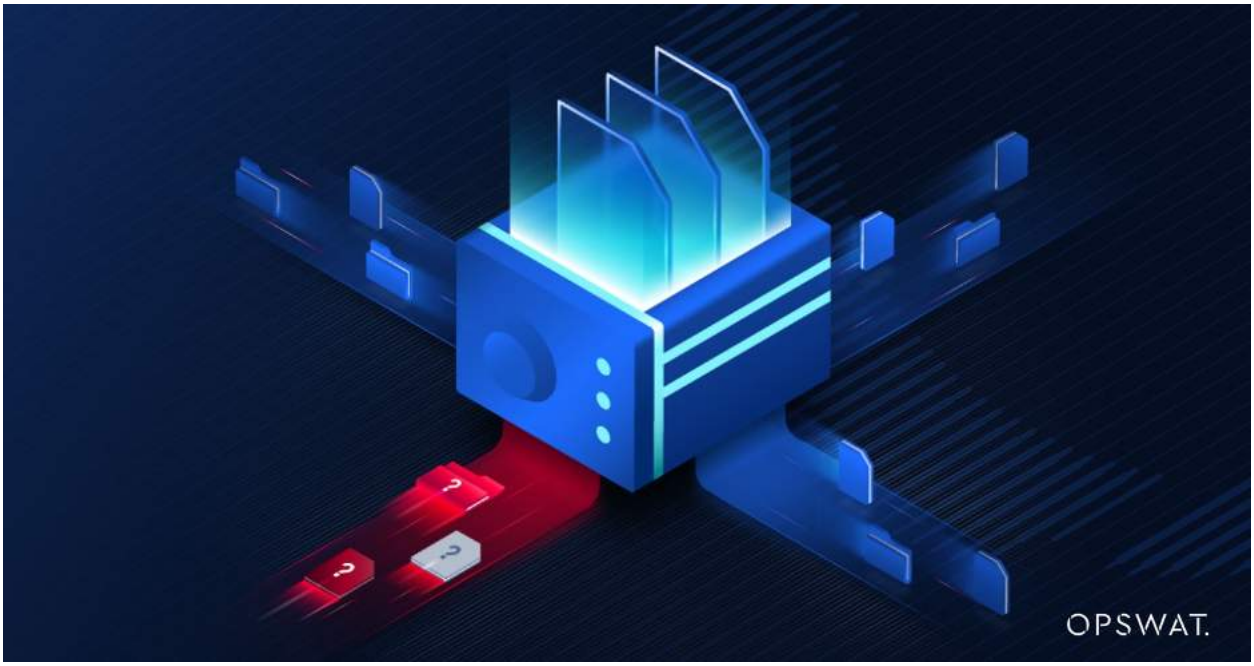
保護資料傳輸

EnergyCo 負責在全美生產和分配電力和化石燃料產品。他們的營運仰賴於持續的資料傳輸，傳輸過程通常會經過員工和承包商之手。其隔離網路系統需要不斷地從員工和承包商設備下載資料、進行系統更新、維護和升級。

為了降低惡意軟體透過檔案傳輸滲透到 EnergyCo 系統的風險，該公司採用了OPSWAT的零信任方法，可以對資料傳輸進行嚴格的控管。這種戰略方法不僅使他們能夠滿足不斷更新的 NERC CIP 要求，尤其是關於 TCA（瞬態網路資產）和可靠性標準的要求；更使得 EnergyCo 能夠積極應對新興的法規，例如美國的大容量電力行政命令 （#13929）。

OPSWAT的解決方案： MetaDefender Managed File Transfer

OPSWAT以保護美國98%的核能設施安全而聞名，因此被EnergyCo選為網路安全合作夥伴。OPSWAT無可挑剔的口碑，是合作過且從中獲益的核能設施認可的，因此才促成了本次與 EnergyCo 的合作。EnergyCo 試圖複製其核能同行所享有的高水準網路安全，從而選擇部署 OPSWAT的跨域解決方案 MetaDefender Managed File Transfer。



MetaDefender Managed File Transfer 提供以下優勢：

透過集中管理進行檔案傳輸

- 集中管理配置，以妥善管理內部和外部使用者以及網路之間的大型檔案傳輸安全
- 無需管理多個檔案傳輸管理供應商
- 減少大量整合

內建安全性

- Deep CDR（深度檔案無毒化）和即時沙箱秉持著零信任原則，不允許未經掃描的檔案進入
- 使用掃描工作流進程預防惡意軟體爆發
- 30多種反惡意軟體引擎可在外部檔案傳輸至內部期間，防止零時差惡意軟體侵害
- 確保檔案型漏洞評估
- 在不犧牲可用性的情況下提供強大的安全性
- 防止外部單位利用有漏洞的可執行檔案來擴大攻擊面。

透過精密自動化來提高效率

- M2M之間的自動化消除了手動傳輸的需求，並簡化了業務流程
- 手動臨時檔案（ad-hoc file）共用功能
- 精細控制系統和用戶之間的自動化資料傳輸

遵守資料保護控制措施

- 主動式 DLP（資料外洩防護）能支援合規性需求並保護聲譽
- 支援靜態加密和傳輸中加密
- 精細的批准流程支援角色型操作權限控管和審計軌跡。

EnergyCo 整合了 MetaDefender Managed File Transfer 以增強安全性並提升組織內部的檔案檢索效率。該解決方案可有效防止零時差威脅和未知的檔案型威脅，並結合了必要的檔案傳輸管理功能與OPSWAT 威脅預防的尖端技術。它確保了在低安全性到高安全性的網路之間，能夠可靠地、易於管理地且安全地傳輸檔案。

控制風險：統一一致的安全流程

EnergyCo 積極主動的網路安全方案為業界樹立了新標準。隨著能源產業不斷發展，像 EnergyCo 這樣的組織必須優先考慮安全性，以保護其營運順利並能適應不斷變化的監管環境。OPSWAT的 MetaDefender Managed File Transfer，顯現了創新技術如何保護關鍵基礎設施免於新興威脅侵擾。

想了解更多關於 OPSWAT的 MetaDefender Managed File Transfer 如何保護您的關鍵基礎設施，現在就聯繫 OPSWAT 專家。