OPSWAT.

金融服務業實際案例

關鍵性基礎架構防護

客戶簡介

金融再保險公司 Swiss Reinsurance Company Ltd 是世界領先的再保險、保險和其他形式基於保險的風險轉移供應商之一。

網路安全對於保護瑞士再保險(Swiss Re) 公司所管理的大量客戶個人數據至關重要。Swiss Re還需要確保遵守現有和新興的金融服務法規和網路安全標準，包括用於預防金融犯罪的瑞士金融市場監督管理局 (FINMA) 和確保數據隱私的《一般資料保護規範》 (EU GDPR)。

01

保護網路—由合作夥伴或客戶在網路邊緣上載的任何檔案，在其到達他們的網路應用程式之前先進行掃描

02

確保客戶個人資料的安全性符合瑞士金融市場監督管理局 (FINMA) 和《一般資料保護規範》(GDPR) 的規定

03

自動化且容易整合—能輕鬆配置、設定並管理部署

挑戰

保證客戶在世界各地資料上傳的安全性

為確保客戶、合作夥伴及員工遞交和傳輸電子檔案的便利性，瑞士再保險 (Swiss Re) 公司建立了可輕鬆上載檔案的入口網站和應用程式。此舉帶來的風險是，受感染的檔案可能會經由他們的一個網路應用程式而進入其安全的網路。為降低安全性和合規性的風險，Swiss Re 需要確保上載的檔案不包含任何惡意的內容。他們最主要的要求，是允許從任何外部來源傳入的檔案，並使其 100% 安全可用，而不至於增加延遲、影響工作流程或檔案的可取用性。此外，該解決方案需要滿足監管的規定、具有成本效益，並且能在整個企業中迅速擴充。

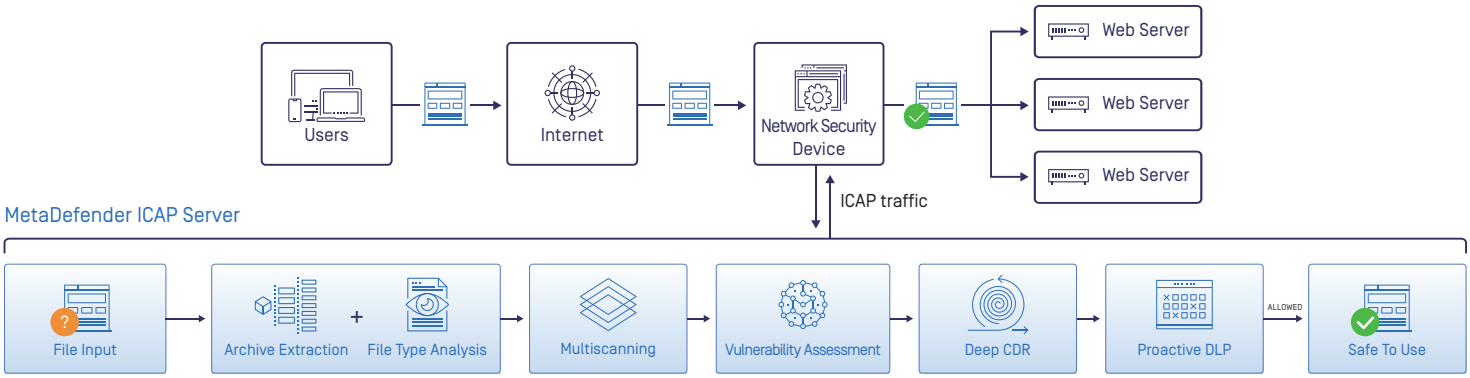
選擇標準

與他們微服務架構的相容性在選擇過程中扮演著重大的角色—他們需要一個能夠在其 Azure/Kubernetes 環境中輕鬆部署的解決方案。OPSWAT MetaDefender + ICAP 伺服器平台為容器化的部署賦予緊密的支援，提供強大且全方位的防護功能，以保護 Swiss Re 的關鍵性資料流量。

除了支援他們目前的架構以外，他們還需要該解決方案能夠符合其未來的技術路線。透過對 NGINX/NGINX Plus 入口控制器 (Ingress Controller) 增加原生支援，諸如 Swiss Re 等的客戶將能夠把此防護能力延展到數個整合點，最終的結果是一個靈活、容易使用且統一的安全性體驗。

為保護其高度敏感性的客戶資料，Swiss Re 需要傳統解決方案中無法提供的先進功能。

多重掃描技術利用數個防毒引擎掃描檔案 (包括數個層級的嵌套檔案(Nested Archive))，以達到最高的偵測率。處理過程沒有延遲 (在幾毫秒內)，而且系統管理員會即時收到潛在威脅的警告。



解決方案

MetaDefender 為 Swiss Re 的網路提供防護，使其免於惡意檔案上傳的攻擊

Swiss Re 在其 Azure 容器例項 (Azure Container Instances, ACI) 之上部署 OPSWAT MetaDefender Core ICAP 伺服器，並將其與 API 閘道整合。他們搭配使用 MetaDefender Core，可驗證所有傳入的檔案並掃描惡意軟體，以保護其基礎架構免受惡意負載的攻擊和敏感性資料的遺失。此技術組合為 Swiss Re 提供可擴充的高效防護，預防邊緣處的惡意流量到達該公司的網路應用程式。

Swiss Re 借助 MetaDefender 所得到的是：

- 透過單一虛擬管理平台而縮短的回應時間—在「MetaDefender Core 和 MetaDefender ICAP 伺服器」之間統一的平台讓該公司能緊密地監控威脅，並對其做出回應。由於資訊隨時可用，因此可以快速將任何潛在的威脅做分類。
- 進階的惡意軟體偵測和防護— OPSWAT 專有的多重掃描技術利用數個防毒引擎同步掃描每個檔案，以偵測惡意軟體 (利用特徵碼、啟發法 (Heuristics)、NGAV 和機器學習)，能達到 99% 以上的偵測率。
- 幾分鐘內就能部署隨插即用的工具組—OPSWAT 的MetaDefender ICAP 伺服器能迅速地與頂級的應用服務傳遞控制器(ADC)、網路應用程式防火牆 (WAF)、負載平衡器 (Load Balancer)、代理伺服器等作整合。

成效

快速的部署、高效能和可擴充性可大幅地節省總體成本

Swiss Re 因此獲得的效益包括：

- 可擴充的網路應用程式安全性—隨著該公司擴大足跡並在環境中加入新的應用程式，他們也可以有自信地導入 OPSWAT 技術，以保護這些應用程式的安全。
- 企業級的效能—該公司能利用 OPSWAT 來全面掃描數百萬個檔案，並在其內部的服務層級協定 SLAs 範圍內妥善地提供這些檔案。
- 卓越的服務— OPSWAT 為該公司在建立安全的方法上提供協助和專業的見解，讓他們能有效率地處理其龐大的網路應用程式流量。

Contact OPSWAT

To learn more about how OPSWAT can help improve your critical infrastructure protection, contact us today.

2022.03.08