Networks
Secure Networks at Layer-7

雲世代網站應用防火牆

InstantWAF

VMware
虛擬版

阻擋OWASP十大攻擊已不足
結合國際威脅情資，定位威脅來源

■ 雲世代的隱憂：阻擋OWASP十大攻擊已不足

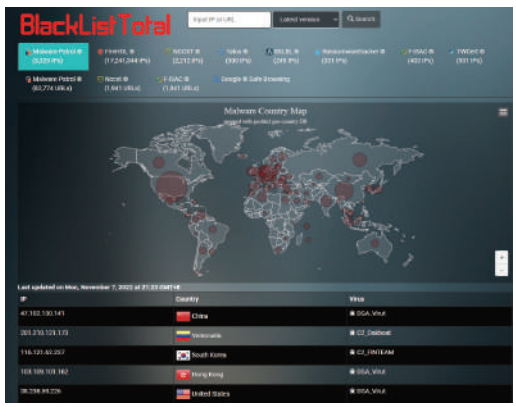
美國聯邦眾議院議長於2022/8/2率領美國眾議院國會訪問團來臺訪問，引發對岸高度不滿，不只進行軍演，網路攻擊更是持續長達9天。這些攻擊手法大致可區分為:分散式阻斷服務(DDoS)攻擊、內容置換(Deface)，以及幾可亂真的假訊息等。

■ 雲世代WAF: 內容結合國際情資單位聯合防禦

網頁遭置換或竄改(Web Defacement)的攻擊手法，主要是系統遭駭客入侵後，取得系統管理員權限，以進行更換網頁的手法，通常網站會遭受駭客置換網頁上傳惡意程式(WebShell)。漏洞通常是網站頁面提供了上傳功能，例如大頭貼、檔案等等，駭客透過殭屍網路，利用經過偽裝副檔名的惡意程式，騙取系統的認證，待順利將惡意程式上傳至系統內部時，即遠端將惡意程式呼叫起來，進而取得系統管理員權限的帳號，以達到控制系統的目的。當今OWASP的前十大攻擊類型之外，仍有許多漏洞可被殭屍網路滲透。

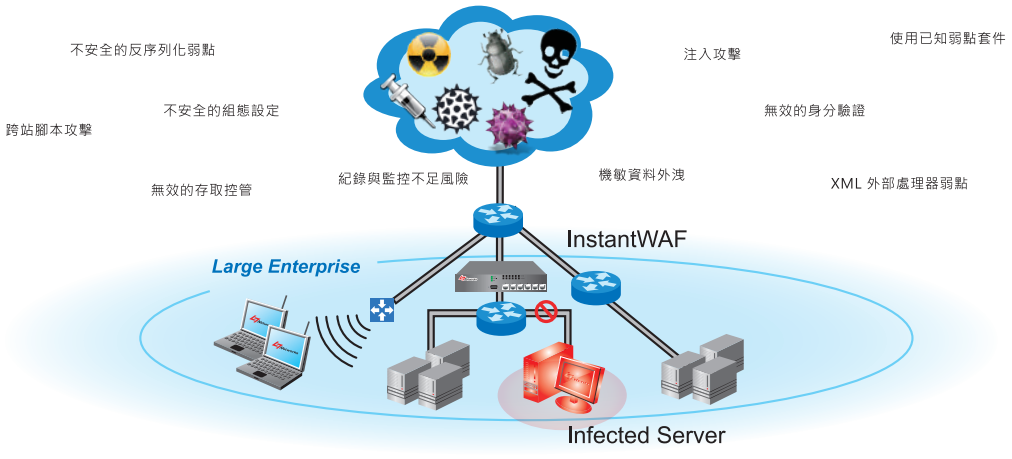
■ 內建BlacklistTotal整合MalwarePatrol/NCCST/F-ISAC/Talos/FireHOL/Abuse國際情資

內建BlacklistTotal情資平台的整合資料庫，內含Malware Patrol、NCCST、F-ISAC、TWCERT、Talos、FireHOL、Abuse、SSLBL等情資單位黑名單，特別針對勒索病毒變種所常用的中繼站，可一網打盡。自動更新政府必要阻擋的計服中心黑名單，不需人工輸入，省時省力。若選購Anti-DDoS模組，可進一步清可進一步清洗Syn/UDP/ICMP flooding流量、限制單一IP來訪本地的連線數與頻寬、緊急時自動阻擋擋國外IP來訪



■ 內建Application Delievery功能

InstantWAF內建server load balancer與reverse proxy功能，並能匯入SSL憑證解密流量後，將解密完的http明碼經過檢查後，送往正確的後端server。後端server的健康狀態，可由InstantWAF監看，若有負載太高的情況，自動跳開該台server將服務要求送往其他負載較低的server。可對http的header進行rewrite、insert等動作。



Malware Patrol 勒索情報網

Talos CISCO 威脅情報網

NCCST 國家資通安全會報 技術服務中心

FireHOL 惡意IP情報網

ABUSE.ch 威脅情報網

建議售價: 每Mbps $3,300
每年維護: 每Mbps $750