ASF 系列 WAF & DDoS

關鍵應用的關鍵安全性

Array Web Application Firewall應用防火牆爲保護關鍵業務資源提供了靈活而精確的工具。ASF 通常與負載平衡和應用交付解決方案一起部署，可檢測和阻止攻擊，包括前 10 名OWASP、WASC、第 7 層 DDoS 和zero-day攻擊，具有精確的定位。它能確保各類應用、API、用戶和基礎設施不間斷的安全性，同時支持遵守包括 PCI DSS 在內的安全標準。

每個 ASF Web 應用防火牆都提供了一套全面的保護模組和安全引擎，可防禦一系列客戶端、伺服器端、自動和手動攻擊。 ASI 系列提供實體或虛擬版本，亦有各種公共雲端版本，非常適合需要深入防禦網路防火牆、入侵檢測和預防系統或網路監控無法檢測到的應用級攻擊的企業。

保護Web應用及API

Array Web 應用防火牆爲企業提供了一種靈活而精確的工具，得以全面性的保護應用程式、API、用戶和基礎設施免受 Web 攻擊和zero-day漏洞攻擊。

智慧偵測

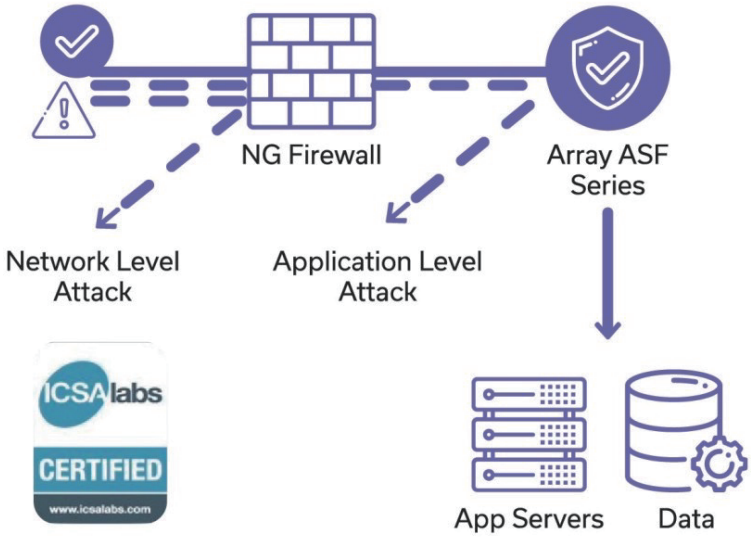
網路威脅情報
全面的威脅記錄和監控

自動學習

行爲分析
動態刷新防禦設定檔

部署模式

橋接模式
路由模式
TAP 模式



領先的WAF功能

主動 DDOS 防禦

經過行爲分析進行剖析，可提高應用安全性並預測攻擊將如何展開。

自動阻止ZERO-DAY攻擊

基於機器學習運算法的多種技術結合起來，可標記任何異常並自動阻止威脅。

針對性保護

內建安全掃描器可檢測應用來源碼中的漏洞並阻止攻擊企圖。

防止對最終用戶的攻擊

由於客戶端安全模組數據屏蔽和精細存取設置，應用程式用戶可以保持安全。

防止機器人攻擊的精確保護

爲用戶建立行爲模式可以輕鬆識別機器人並阻止自動攻擊，而不會減慢合法流量。

網路和行動 API 的完全安全

經過分析 JSON 和 XLM 數據以及協力廠商整合來阻止對 Web 和行動 API 的威脅。

安全的應用交付

與 Array 負載平衡一起部署以建立端點到端點的應用交付網路解決方案。

實體、虛擬和雲端部署

提供實體機或虛擬版本，亦提供在AWS、Azure和 Google Cloud Platform 上運作的雲端原生實例

成功導入WSF案例

面臨挑戰

作爲擁有廣泛線上服務的院級政府單位，嚴峻的資安問題是最大的挑戰，我們的網站和應用程式經常受到各種惡意攻擊，包括跨站腳本(XSS)攻擊、QL注入攻擊和應用程式層面的其他威脅。不僅對我們的資訊安全造成了威脅，還嚴重影響用戶的使用體驗和信任度。

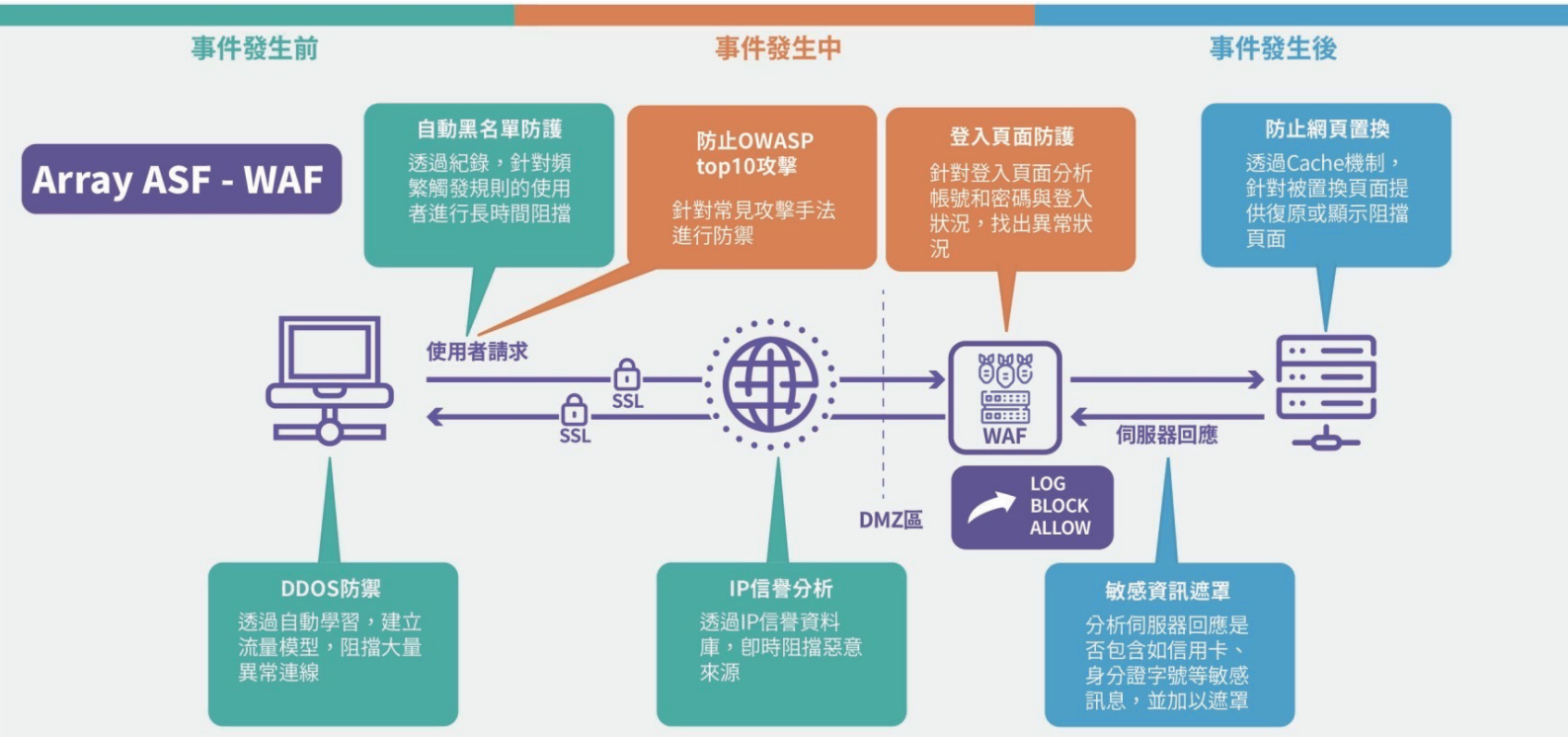
導入方案

爲了有效應對挑戰，我們決定導入Web應用程式防火牆(WAF)解決方案。選擇了擁有豐富經驗和可靠技術的供應商合作，最能確保我們的網站與應用程式能得到最佳的保護。

達成效益

WAF有效地阻止大多數惡意攻擊，包括XSS攻擊和SQL注入攻擊，從而保護了用戶的個人資訊和機密數據。攻擊減少了，我們的網站和應用程式的可用性和性能都得到了提升，順暢的網路通訊也提高了客戶的滿意度與忠誠度。WAF能自動阻止大多數攻擊更有助於降低維護管理成本，再也不需要花費大量的時間和資源來應對這些攻擊。

綜上所述，導入WAF是一個明智的決定，我們看到了明顯的效益和改善，和供應商的持續合作也將確保我們的網站與應用程式固若金湯。



台灣代理 定承資訊股份有限公司
電話：(02)8228-7155 傳真：(02)8227-8508
地址：235603新北市中和區中正路700號15樓之6