TSM WAF 網站應用程式防火牆：智慧、精準、多維度的全方位網站防護解決方案

產品型錄

一、 產品概述：新世代的應用層安全守護者

在數位化浪潮下，網站與 Web 應用程式已成為企業營運的核心。然而，隨之而來的 SQL 注入、跨站腳本（XSS）、零日攻擊等網路威脅也日益猖獗，傳統的防火牆難以應對這些針對應用層邏輯的複雜攻擊。

TSM WAF（Web Application Firewall）是一款專為現代化企業設計的智慧型網站應用程式防火牆。我們不僅提供業界標準的攻擊防禦能力，更創新地整合了**「外傳資料流量管控」**與**「檔案鎖定監控」**兩大獨特功能，打造出超越傳統 WAF 的多維度縱深防禦體系。無論您的應用部署在實體機房、私有雲或公有雲，TSM WAF 都能以其獨特的 **Agent Mode** 與 **Reverse Proxy Mode** 雙模式架構，融入您的 IT 環境，為您的數位資產提供最堅實、最靈活的安全屏障。

二、 核心功能亮點

1. 業界標準 WAF 防護能力

TSM WAF 內建強大的核心防護引擎，能有效抵禦 OWASP Top 10 等常見的網路攻擊：

- **SQL 注入防護：** 精準偵測並阻斷惡意的 SQL 查詢語句，保護資料庫安全。
- **跨站腳本（XSS）防護：** 過濾惡意腳本，防止用戶端資料遭竊取或網頁被篡改。
- **遠端程式碼執行阻斷：** 防範攻擊者利用漏洞在伺服器上執行任意代碼。
- **其他威脅防護：** 包含本地檔案包含（LFI）、遠端文件包含（RFI）、命令注入等全面性防護。
- **可自訂規則集：** 管理員可根據業務需求，輕鬆啟用、停用或微調防護規則，實現精細化管控。

2.【獨家特點】智慧外傳流量限制功能

異常的流量輸出往往是資料洩漏的前兆，例如駭客竊取大量機密或客戶資料後，經由網站服務器來分批大量傳輸回 C&C (C2 控制器)。TSM WAF 的智慧外傳流量限制功能，能從傳輸層面提前預警與阻斷。

- **自動化連線切斷：** 可針對單一 HTTP(S) 請求或連話期設定外傳流量上限。當傳輸的數據量超過預設閾值時，系統將自動切斷該連線有效防止機敏資料被竊。
- **即時告警通知：** 觸發流量限制的同時，系統會立即向指定的管理員或安全團隊發送告警電子郵件，內容包含觸發時間、來源 IP、目標 URL 等關鍵資訊，便於團隊第一時間進行事件分析與應變。
- **靈活策略配置：** 可針對不同路徑（URL）或網頁服務設置個別化的流量限制，。

3.【獨家特點】檔案與目錄鎖定功能

網站竄改（Defacement）和惡意程式植入是常見的攻擊結果。TSM WAF 的檔案鎖定功能能從根源上杜絕此類威脅。

- **核心檔案完整性保護：** 對網站根目錄、系統設定檔、關鍵程式庫等核心檔案與資料夾進行鎖定監控。
- **即時變更偵測與阻擋：** 一旦偵測到未經授權的寫入、修改或刪除行為，系統會立即阻止該操作並發送告警通知 email。
- **白名單機制：** 對於需要正常更新的項目（如內容管理系統的媒體上傳目錄、快取目錄），可設置白名單及檔名過濾機制確保不該存在的檔案不能存在。

4. 雙部署模式：無縫適應任何環境

TSM WAF 提供兩種部署模式，賦予企業最大的架構彈性。

- Agent Mode（代理模式）：
  - **簡潔輕量：** 以軟體 Agent 的形式直接安裝在 Web 伺服器（ Apache, Nginx, IIS ）上。

    - **高效能低延遲：** 由於防護發生在本機，無需將流量轉向其他節點，特別適合對延遲極為敏感的應用或內部系統。
    - **易於管理：** 可透過中央管理平台統一收集日誌，簡化維運複雜度。
- **Reverse Proxy Mode（反向代理模式）：**
    - **集中式防護：** 作為一個獨立的安全網關，所有外部流量都先經過 TSM WAF 進行清洗與過濾，再轉發至後端的 Web 伺服器群。
    - **隱藏後端架構：** 有效遮蔽真實伺服器的資訊，提升攻擊難度。
    - **易於橫向擴展：** 適合大型網站或微服務架構，可輕鬆進行水平擴展以應對高流量負載。

三、 產品優勢與價值

- **防禦縱深化：** 結合「應用層攻擊檢測」、「流量行為分析」、「檔案完整性監控」三層防護，提供立體式的安全保障。
- **部署靈活化：** 獨特的雙模式設計，可根據現有 IT 架構選擇最合適的方案，保護既有投資。
- **高性價比：** 單一產品整合多項進階功能，無需採購多套零散工具，有效節省總體擁有成本（TCO）。
- **合規性輔助：** 強大的防護與詳盡的稽核日誌，有助於企業滿足 GDPR、PCI DSS 等國內外資安法規要求。

四、 適用場景

- **電子商務平台：** 保護用戶個資與交易數據，防範網頁竄改導致的品牌信譽損害。
- **金融服務機構：** 為網路銀行等各項金融服務提供最高等級的安全防護。
- **政府與教育單位：** 確保官網與服務系統的穩定性與可靠性，防止敏感資訊外洩。
- **任何擁有官方網站或 Web API 的企業：** 防範資料洩露、服務中斷等營運風險。

五、 技術規格摘要

- **部署模式：** Agent Mode（支援主流 Web Server）、Reverse Proxy Mode
- **防護能力：** OWASP Top 10、自訂攻擊規則、虛擬修補
- **獨特功能：** 外傳流量限制、檔案目錄鎖定
- **日誌與報告：** 完整存取日誌、安全事件日誌，支援自訂報表生成
- **通知機制：** 電子郵件告警

結語

在網路威脅日益複雜的今天，被動防禦已不足以保障企業安全。TSM WAF 以主動、智慧且全面的設計理念，為您的網站與應用程式築起一道動態的智慧防線。無論是阻擋外部攻擊，還是管控內部異常行為，TSM WAF 都是您最值得信賴的安全合作夥伴。

立即聯絡我們的銷售團隊，為您的企業安排一場專屬的產品演示與安全評估，體驗 TSM WAF 如何為您的數位業務保駕護航。

TSM WAF™企業版產品功能表	
網頁伺服器記錄	網頁存取紀錄，含網頁執行時間等相關細節。
	HTTP 200 網頁輸出記錄。
	HTTP 200 使用記錄、軌跡資料及證據保存。
	攻擊偵測紀錄。
	HTTP 500 錯誤畫面記錄。
	HTTP 500 錯誤訊息可提供系統開發者重要訊息供開發者修正程式，提高系統穩定度。
稽核及損害控制	檢查非法連結及其來源：可檢視詳細非法連結來源及其網址，所傳送之攻擊指令等細節。
	輸出網頁內容條件檢索。
安全	支援 SSL, HTTP/2 及 TLS1.2/TLS1.3 資料傳輸使用 AES 256 及 RSA 2048bit 加密運算。
	HTTP XML Web Service 防護：保護 xml web service 避免未授權網址存取 XML Web Service API。
效能	支援 IPv4 及 IPv6。
	高效能規則引擎，高效能模組，支援關鍵字及 regular expression 正則表示法過濾規則。
	網頁監視伺服器搭配 WEB X-RAY 系統，支援後端資料庫 MySQL/MariaDB。
	高效能資料查詢介面。
	擴充性(Scalability)：分散式架構，企業版可大量橫向擴充(scale out)網頁伺服器 Agent，效能不受伺服器數量影響。
網頁攻擊偵測	HighBit Shell Code 阻擋。
	Parent Path 阻擋。
	Directory Traversal 阻擋。
	Hex Encoding 阻擋。
	SQL Injection、XSS(Cross Site Scripting)、CSRF(Cross-Site Request Forgery) 阻擋。
	即時 Email 警示訊息通知。
	白名單(White List)設定。起始網址(Start URL)設定。拒絕網址(Deny URL)設定。
	HTTP Header 偵測防護。
	根據 URL 自訂防禦與偵測規則(Per URL rule support)。
	自訂輸入特徵檢查規則(Input Pattern Rule)。
	掃描 POST 資料。
	掃描 GET 資料 (URL Scan)。
支援平台	支援作業系統與版本： 本機安裝支援: Linux Ubuntu 24.04LTS，Alma Linux 9/10， Apache 2.4，Windows 2016~2025/IIS x64，Nginx (1.18 以上，需洽詢後方能支援)。 Reverse Proxy Mode: TSM WAF™ 使用 Reverse Proxy Mode 時，後端防護之 Web server 需支援 reverse proxy mode。 企業版記錄基本空間 10 TB。XRAY 可記錄資料量可視需要規劃，如需更多記錄資料可另行洽談規劃不受上限影響。
	軟體 Agent 網頁伺服器硬體基本需求: Intel CPU x 2 RAM: 4+GB 檔案目錄鎖定功能 Agent Mode 適用，Reverse Proxy Mode 不適用。 Reverse Proxy Mode 硬體基本需求: Intel CPU x2 RAM: 32+GB (視實際流量需求由雙方討論規劃) Storage: 1+TB

TSM Software 小松鼠軟體

TSM Software Technology, Inc.
小松鼠軟體有限公司
新北市中和區景平路 288 號 13 樓之 15
Tel: +886-2-2941-5500
http://www.tsmst.com