Data Sheet

WAPPLES

The Logical Web Application API Protection

WAPPLES 網頁應用程式和 API 保護 (WAAP) 使用AI邏輯檢測引擎來分析 HTTP 和 HTTPS 流量內容，保護您的網頁應用程式、API和行動APP，避免遭受惡意攻擊。 WAPPLES 解決方案能有效保護應用程式免受各種零時差攻擊；防止敏感數據洩露、網站污損、殭屍網路或DDoS攻擊，協助企業建構優於法規的嚴謹保護。

功能特色

- 具有預定義規則集的AI邏輯檢測引擎 COCEP™
- 防護範圍涵蓋 OWASP Top 10 和 OWASP Top 10 API
- 使用各種LB算法進行流量負載平衡
- 透過虛擬補丁程式快速修復漏洞
- 實用的多合一憑證策略
- 可在本地部署也支援虛擬設備或雲端基礎的 SaaS (軟體就是服務)
- 具備in-line (通透)、Reverse Proxy (反向代理)、Transparent Reverse Proxy (透明反向代理)及Active-Active (主動-主動)、Active-Passive (主動-被動)等部署模式

邏輯檢測引擎 COCEP™

WAPPLES 的專利檢測引擎 COCEP™，不仰賴電子簽章資料庫無需漫長學習歷程；利用網路攻擊邏輯精選39種檢測邏輯規則，完整的邏輯規則涵蓋了已知和零時差漏洞的所有攻擊手法，包括OWASP Top 10 & OWASP TOP 10 API 。

Web應用程式、API和行動APP的進階防禦

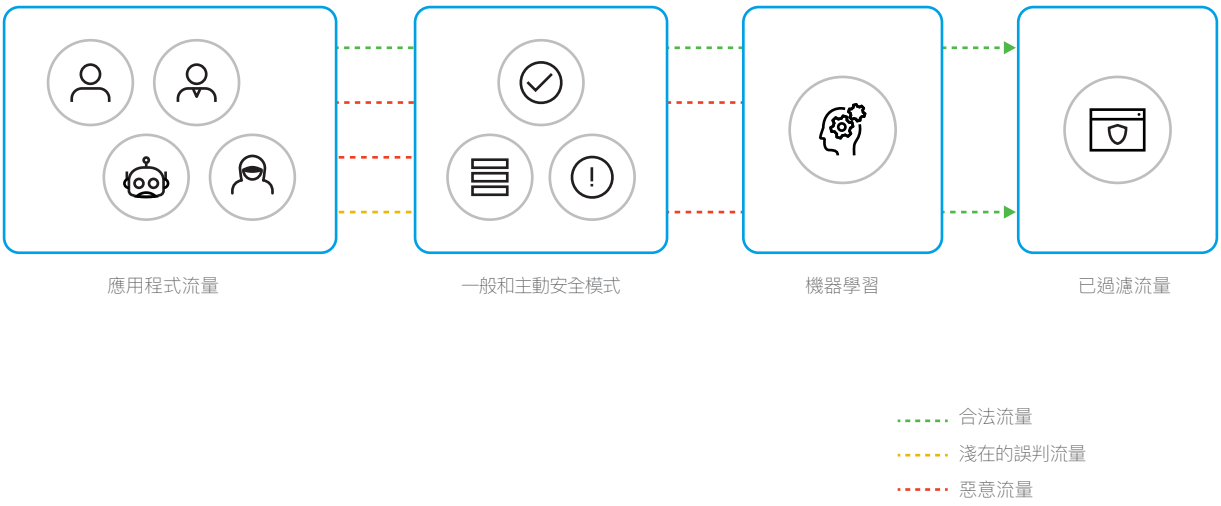
為提高整體效率，應用程式的使用漸漸轉變為API環境，如Web / XML / JSON。 但是；當應用程式環境更改時，通過API發出的威脅也會增加。 而WAPPLES的COCEP™引擎會透過專用API解析器/架構來阻止這類威脅。

有效防禦惡意殭屍網路和DDoS攻擊

惡意用戶會使用自動化工具或惡意殭屍網路的方式，匿名進入攻擊目標的企業網站；而透過WAPPLES防護的企業網站，能啟動指紋識別、驗證碼(CAPTCHA)和各種行為模式檢測技術來阻止惡意殭屍網路的可疑訪問，有效的保護企業網站和其相關重要的數據。

極低的誤判率

WAPPLES的COCEP™引擎不僅在阻止各種已知和未知的攻擊模式方面非常有效，而且邏輯規則不會影響安全流量。 WAPPLES的誤判率幾乎為零，在安全及性能上都有出色優秀的表現。



簡便又強大的登入管理

不僅WCC的管理員帳戶，所有的設定和組態都可以透過WAPPLES控制中心（WCC）受到安全地保護。管理員可以建立自己專用的登錄認證，或輕鬆地透過與Active Directory整合來登入。WAPPLES中控台登入可增加OTP驗證程序；雙重驗證有效保護。

具有自我診斷和定期檢查功能，使管理更簡單

WAPPLES擁有預設的安全規則策略，管理者可以在圖形界面上輕鬆部署和管理WAAP。自我診斷功能可以檢測並警告來自系統及資源相關的潛在問題。WAPPLES能夠透過虛擬修補，立即修復漏洞。

FEATURES

網站保護 Web Protection

- HTTP合規性驗證 / HTTP Compliance Validation
- 蠻力攻擊 / Brute Force Attack
- Tro 節點封鎖 / Tor Nodes Blocking
- Web Socket 保護 / Web Socket Protection
- 網址加密 / URL Encryption
- OWASP 安全標頭 / OWASP Secure Header

資料外洩防護

- 屏蔽敏感信息 / Masking of Sensitive Information
- 私人數據洩漏 / Private Data Exposure

應用層傳輸

- Layer7 服務負載平衡 / Layer7 Server Load Balancing
- 黏滯會話 / Sticky Session
- HTTP 壓縮 / HTTP Compression
- SSL 卸載 / SSL Offloading
- 支援HTTP/2.0 / HTTP/2.0 Support

應用程序安全保護

- OWASP十大漏洞 / OWASP Top 10 Vulnerabilities
- 注入攻擊 / SQL/NoSQL/LDAP/Xpath Injection
- 伺服器端注入攻擊 / Server-Side Injection
- 應用程式級別 DDOS / Application-level DoS
- 驗證碼和瀏覽器指紋 / CAPTCHA and Browser FingerPrinting
- 虛擬補丁 / Virtual Patching
- 跨網站指令碼攻擊 / Cross Site Scripting
- 跨網站請求偽造 / Cross Site Request Forgery
- 目錄瀏覽 / Path Traversal
- 網頁數據抓取防護 / Web Scraping Protection
- 應用程式 / 伺服器錯誤處理 Application / Server Error Handling
- 遠程/本地文件包含 / Remote/Local File Inclusion
- 參數操縱 / Parameter Manipulation
- Cookie 中毒 / Cookie Poisoning
- 惡意文件上傳 / Malicious File Upload
- 網站竄改 / Website Defacement
- 殭屍網路檢測 / Bot Detection
- 零時差攻擊防護 /Zero-Day Attack Protection

API 保護

- Xml 架構/DoS 保護 / Xml Schema/DoS Protection
- JSON 架構/DoS 保護 / JSON Schema/DoS Protection
- YAML 架構/DoS 保護 / YAML Schema/DoS Protection

部署方式

- 通透模式 / Transparent Inline
- 反向代理模式 / Reverse Proxy
- 透明反向代理模式 / Transparent Reverse Proxy
- 監視(鏡像)模式 / Offline Monitoring (Mirroring)

靈活的檢查控制

- 自定義規則 / Custom Rule
- 預設的安全策略 / Preconfigured Security Policies
- IP信譽檢測 / IP Reputation
- IP地理位置封鎖 / IP Geolocation-based Blocking
- HTTP 標頭控制 / HTTP Header Control
- URL訪問控制 / URL Access Control
- URL / HTML / Base64解碼 / URL/HTML/Base64 Decoding
- 風險評分 / Risk Scoring

其他功能

- 自我診斷和警報 / Self-Diagnostics and Alert
- LDAP / Active Directory 整合 / LDAP/Active Directory Integration
- 控制台具備二階段驗證 / Admin Console Login with 2FA
- 誤判恢復快速 / Fast False Positive Recovery
- SSL / TLS 版本不足和密碼控制 / Weak SSL/TLS Version & Cipher Control
- SSL憑證管理 / SSL Certificate Management
- 支援 IPv6 / IPv6 Ready
- 支援網絡 HSM / Network HSM Support
- 支援 SSL 加速卡 / SSL Accelerator
- 安全的 SSL 密鑰儲存 / Secure SSL Key Storage
- Web訪問管理 / Web Access Management
- 支援用戶端憑證 / Client Certificate Support

管理與報告

- 網頁 / 命令列使用者介面 Web / Command Line User Interface
- 定制報告產出 / Customized Report Generation
- 透過電子郵件自動發送報告 / Automatic Report Delivery Via Email, Etc.
- OWASP Top 10分類報告 / OWASP Top 10 Categorized Report
- REST API
- SNMP、Syslog 和 E-mail 監控
- 即時儀錶板 / Real-time Dashboard
- 集中管理多個設備
- 主動/主動、主動/被動 整合
- 同步策略日誌 / Policy Log Synchronization
- 包含地理位置的日誌記錄和監視

WAPPLES SA

WAPPLES 虛擬設備

WAPPLES SA Web 應用防火牆 (WAF)，可保護企業Web應用程序避免遭受已知漏洞攻擊和零時差攻擊。
WAPPLES SA 除了可以有效阻止SQL注入和跨站點腳本 (XSS) ...等Web攻擊外，
透過專利的 COCEP™ 邏輯檢測引擎，還可以防止數據洩露、網站污損和可疑的機器人攻擊。

WAPPLES SA 為敏感資產提供強大的保護，進而實現客戶信賴的安全服務。

1) COCEP™ ：Contents Classification and Evaluation Processing 內容分類和評估處理

自我診斷功能

為了維護可靠的Web服務，必須及時解決任何阻礙流量的問題。
WAPPLES SA中的自我診斷功能，會對影響服務交付的各種性能狀態進行連續檢查，
並在任何狀態超過最低安全閾值時，自動觸發修復並向管理員發出警報。

WAPPLES SA 的關鍵優勢

- 降低總體營運成本(TCO)
- 高可用性模式，實現穩定的服務
- 借助領先的網絡安全增加網頁信任度
- 使用Layer 7 主機名的多網域NAT
- 廣泛的合作夥伴關係和協作模式
- 支持最新協議 HTTP/2 和 TLS 1.3
- 具備自我診斷功能的即時健康監控
- 可立即設定”自定義規則”修補新漏洞

虛擬設備規格

分類	標準	進階	高階	
型號	WAPPLES SA-50	WAPPLES SA-100	WAPPLES SA-500	WAPPLES SA-1000
流量	100 Mbps	300 Mbps	500 Mbps	1 Gbps
記憶體	4 GB	8 GB	16 GB	32 GB
建議儲存空間	HDD 40 GB	HDD 80 GB	HDD 100 GB	HDD 200 GB
支援 HA	Yes	Yes	Yes	Yes
支援管理程序	Vmware, Hyper-V, Xen Server, Linux KVM			
支援雲端(IaaS)服務	AWS, Microsoft Azure, Google Cloud, Alibaba Cloud			

• 實際使用效能因各別系統配置、硬體規格及網路流量等因素將略有誤差。
• 為了確保WAPPLES SA的性能，請參考以下系統建議：
  – 強烈建議使用搭載Intel CPU的伺服器，因為在搭載AMD和ARM CPU（QEMU64）的伺服器上效能穩定性相對略低。
  – 在KVM-QEMU環境配置”QEMU虛擬CPU（QEMU64)”下可能會出現不穩定的情況，建議配置為Intel CPU。