
OCTOFENCE WAAP
Web Application & API Protection

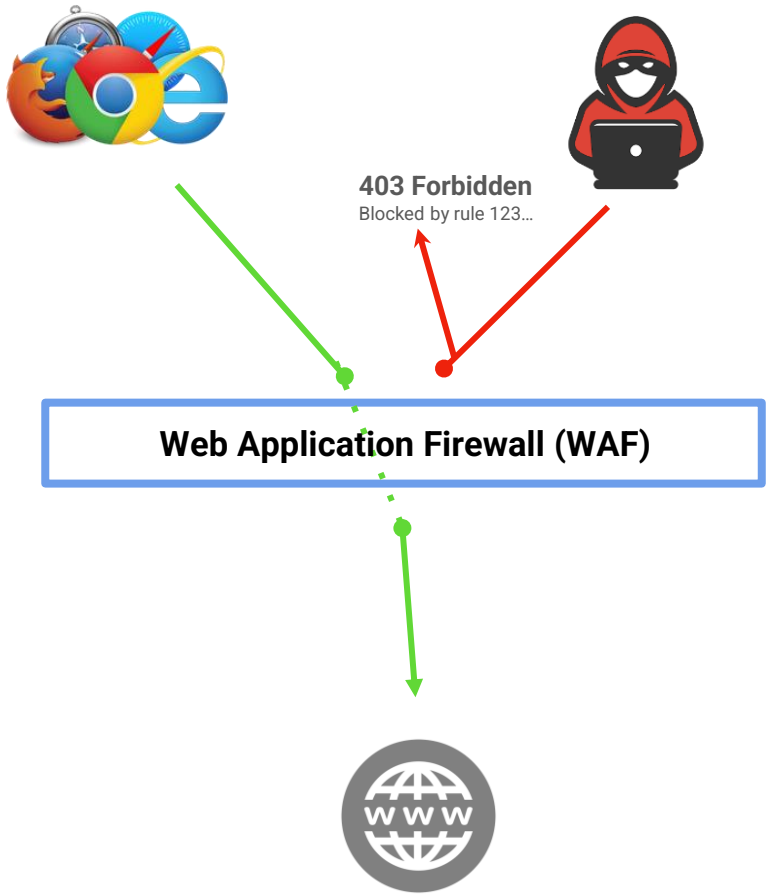
Web **A**pplication **F**irewall (WAF)

Cos'è?

Il **W**eb **A**pplication **F**irewall (WAF)
È uno strumento che **filtra, registra e blocca traffico** HTTP/HTTPS verso un sito o un'applicazione web.

Cosa fa?

Blocca gli attacchi ispezionando tutte le richieste e risposte da e verso un sito. È in grado di capire si tratta un utente che sta effettuando una normale navigazione e permettere l'accesso al sito protetto.



Web
Application
Firewall

OWASP ModSecurity Core Rule Set

OWASP Core Rule Set è un set generico di regole che protegge da molte categorie di attacco elencate nella lista OWASP Top 10 (limitando i falsi positivi) come, ad esempio:

SQL Injection (SQLi)
Cross Site Scripting (XSS)
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
PHP Code Injection
Java Code Injection
HTTPoxy
Shellshock
Unix/Windows Shell Injection
Session Fixation
Scripting/Scanner/Bot Detection
Metadata/Error Leakages

Web
Application
Firewall

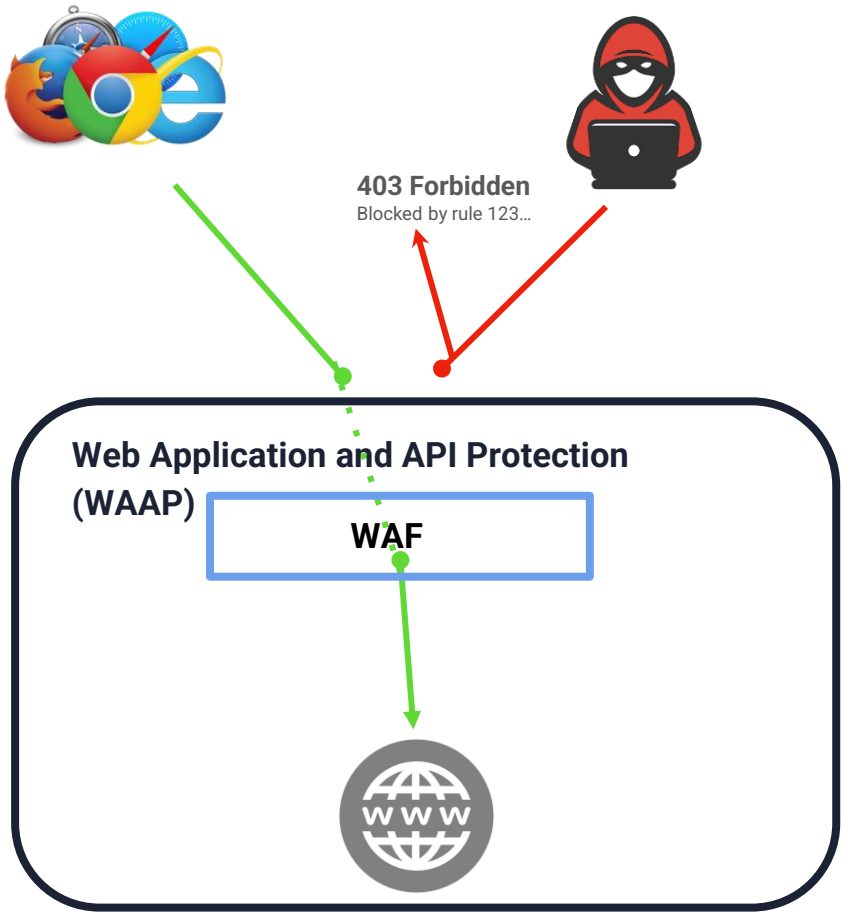
OWASP ModSecurity Core Rule Set

OWASP Core Rule Set viene costantemente aggiornato da un team ristretto di esperti e per questo viene utilizzato da molti grandi vendor e service provider come:

Microsoft Azure
Trustwave
Akamai
GitLab
ORACLE
fastly
CLOUDFLARE
COMODO CYBERSECURITY
sqreen
kemp
verizon

Da WAF a WAAP

SicuraNext ha esteso le feature del WAF ottenendo **Octofence WAAP** (Web Application and API Protection)



in sintesi | **OCTOFENCE WAAP**

OCTOFENCE WAF
Web Application Firewall

BAD BOT DETECTION
Identifica minacce elencate nella “OWASP TOP Automated Threats”

REPUTATION DATABASE
Blocca anonymous browsing, botnet, spammer, abusers, e altre sorgenti malevole

FREE SSL CERTIFICATES
Completa gestione dei certificati SSL senza costi aggiuntivi

VIRTUAL PATCHING
Applica patch su vulnerabilità senza toccare il codice sorgente

DoS L7 PROTECTION
Protegge dalle diverse tipologie di attacco volumetrico a livello applicativo

SECURITY HEADERS
Aumenta la sicurezza degli utenti direttamente sul loro browser

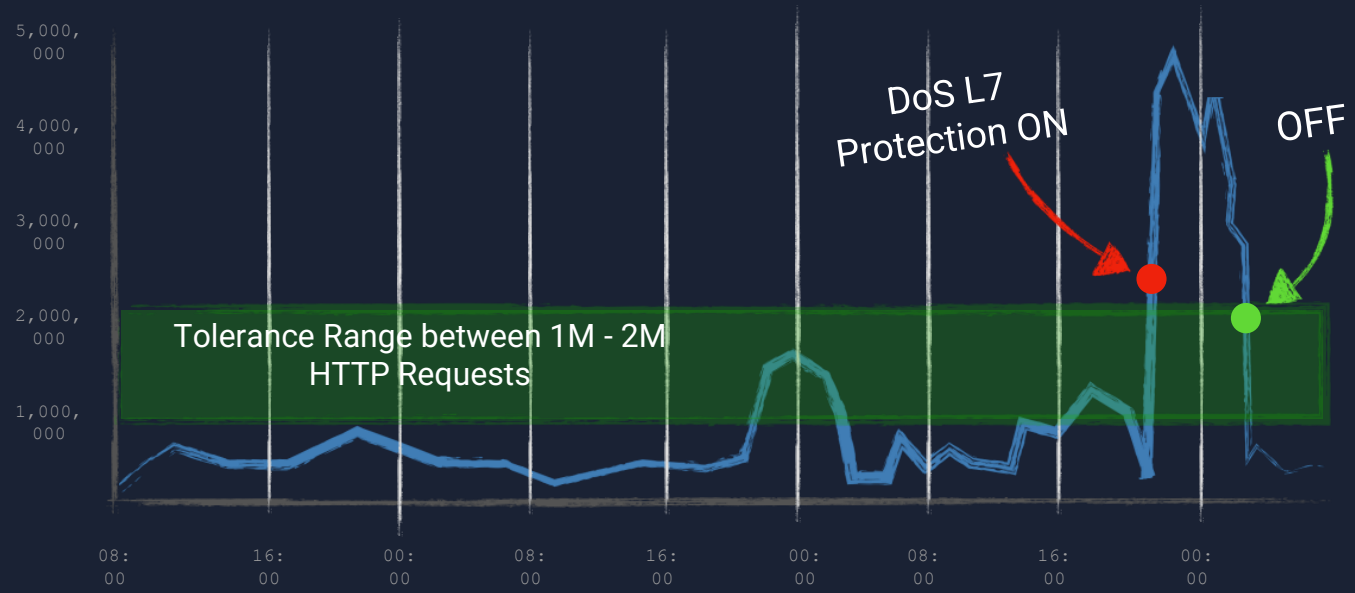
LEAKED PASSWORD
Interagisce con “Have I Been Pwned?” per identificare password in data breach pubblici

CUSTOM RULESET
Utilizzo di un RuleSet dedicato in caso di CMS come WordPress, Joomla, Drupal, ecc…

CACHE & PERFORMANCE
Incrementa le performance dell’applicativo riducendo il ritardo nella risposta utilizzando tecniche di cache, compressione e minificazione dei file

focus | **DoS L7 PROTECTION**

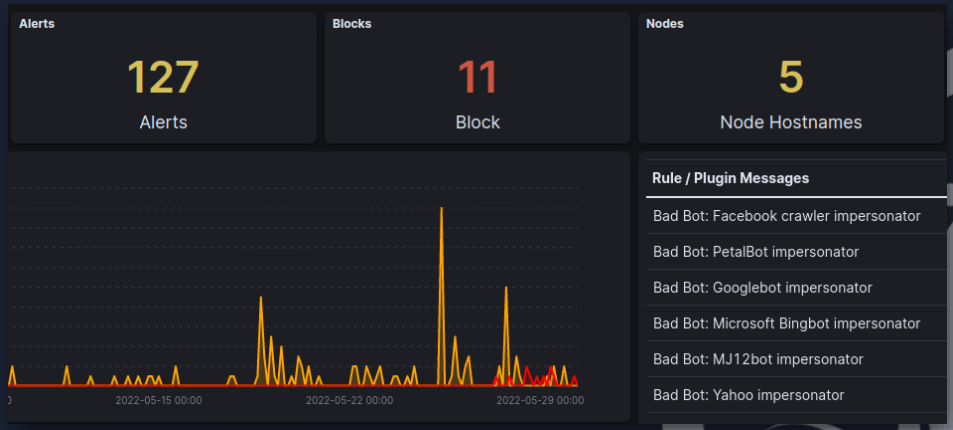
Octofence WAAP DoS L7 Protection si **attiva automaticamente** in base a soglie di traffico predefinite per il cliente. Può generare Challenge JavaScript, Rate Limit o bloccare traffico malevolo e botnet.



focus | **BAD BOT MANAGEMENT**

Octofence WAAP riconosce e blocca bot dalla prima alla quarta generazione, tra cui:

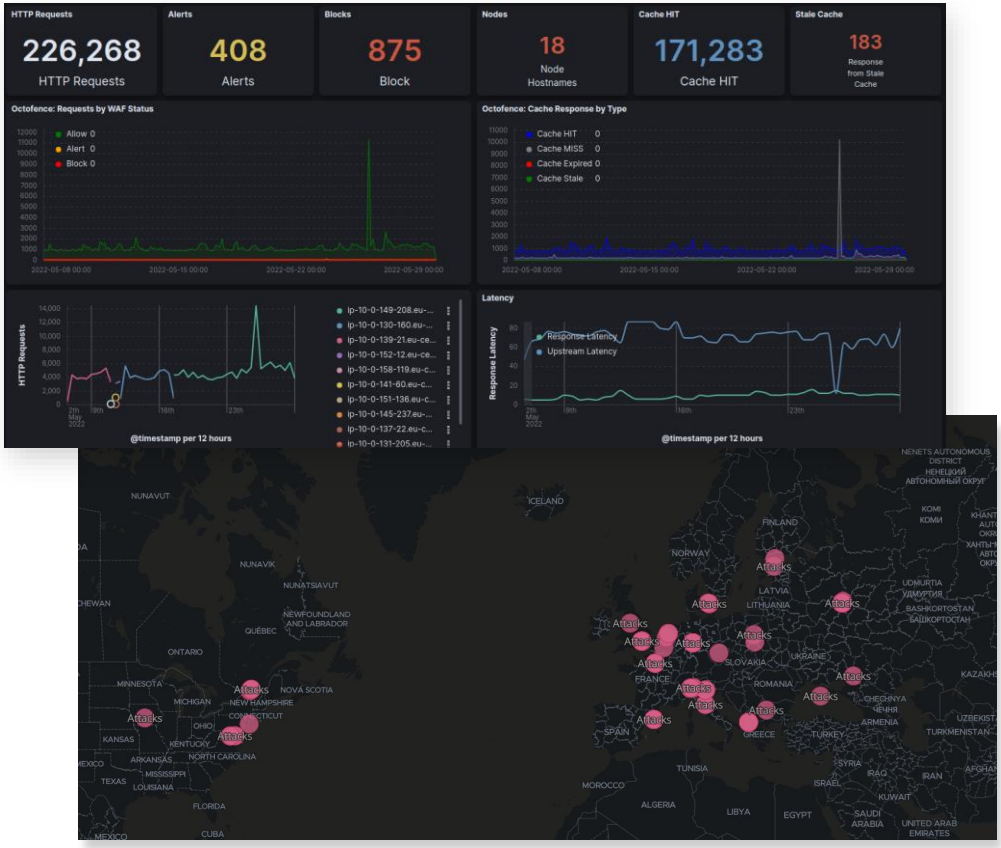
- **Impersonators**
- **Spammers**
- **Token/Coupon Crackers**
- **Brute-Force Attacks**
- **WebScan**



e molte altre categorie elencate nella lista **OWASP Automated Threats**

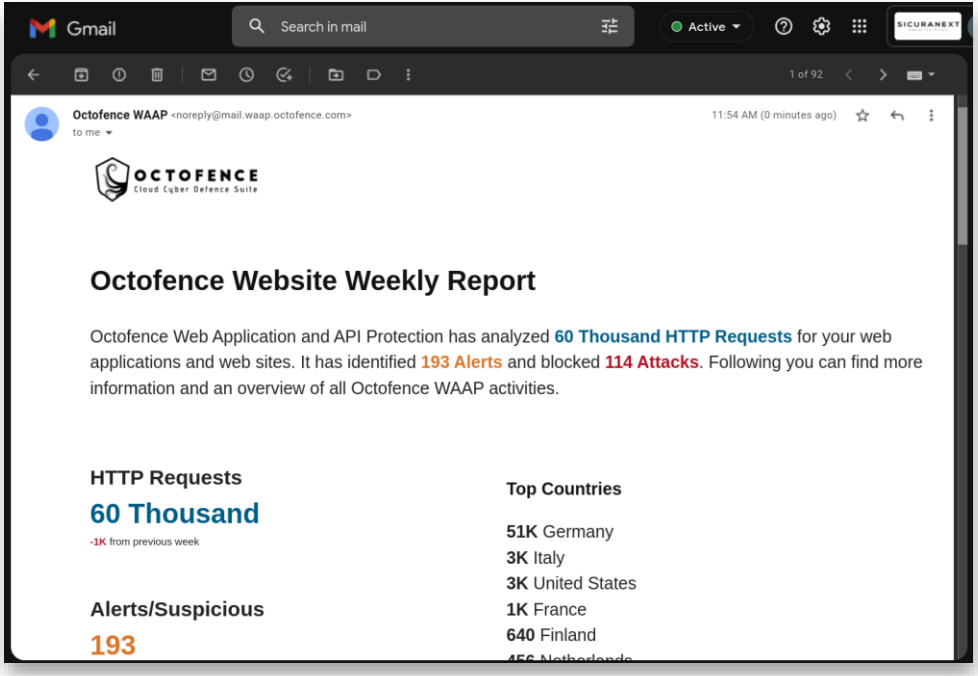
ATTIVAZIONE

- Il servizio si **attiva** con un semplice **change DNS**
- **Gestione certificati SSL gratuita** tramite AWS Certificate Manager
- **Grace Period** di valutazione falsi positivi e tuning delle regole custom
- Blocking Mode



REPORT

- Report personalizzati via e-mail
- Frequenza configurabile
- Analisi di eventi straordinari o degni di nota
- Novità sul servizio e sulle attività del gruppo



vantaggi | **PARTNER**

MINIMUM EFFORT
MAXIMUM RESULTS

- **Esperti a portata di mano** grazie al supporto dedicato attivo 24/7/365
- **Interventi tempestivi** per ridurre al massimo i pericoli e le minacce verso il cliente
- **Tecnologie all'avanguardia** grazie a un costante aggiornamento delle tecnologie utilizzate e delle fonti di informazioni.
- **Risparmio** grazie a un servizio all-in-one ad una frazione del costo rispetto alla formazione di un team e una struttura in-house
- **Monitoraggio e visione a 360°** della sicurezza dell'infrastruttura e dell'immagine aziendale.
- Servizio formato da un team di esperti **gestito totalmente in e dall'Italia**

vantaggi | **CLIENTE**

0 EFFORT
MAXIMUM RESULTS

- **Uptime garantito** in caso di attacco DDoS
- **Riduzione della superficie** di attacco
- **Garanzia della privacy** tramite navigazione protetta
- **Protezione da tutte le vulnerabilità** del web, con aggiunta costante di nuove regole di prevenzione
- **Supporto dedicato** attivo H24

info@sicuranext.net

Corso Vinzaglio 2, 10121, Torino

www.sicuranext.com

www.octofence.com