Barracuda WAF-as-a-Service

Protezione per tutte le app Web, ovunque risieda l'host, in pochi minuti.

L'implementazione di WAF (Web Application Firewall) tradizionali può essere così complessa e causare tanto dispendio di tempo da risultare proibitiva. Alcuni semplicemente installano un WAF in modalità predefinita e non lo configurano mai correttamente, ma così i sistemi rimangono vulnerabili alle minacce basate sulle applicazioni.

È possibile implementare, configurare e rendere subito operativo Barracuda WAF-as-a-Service nel giro di qualche minuto. Grazie ai modelli già predisposti le applicazioni sono immediatamente protette e l'intuitiva interfaccia semplifica l'ottimizzazione di criteri specifici. La protezione DDoS ad ampio spettro assicura la disponibilità continua delle applicazioni e il servizio integrato Barracuda Vulnerability Remediation Service esegue automaticamente la scansione delle applicazioni risolvendo le vulnerabilità.

Semplice ma flessibile

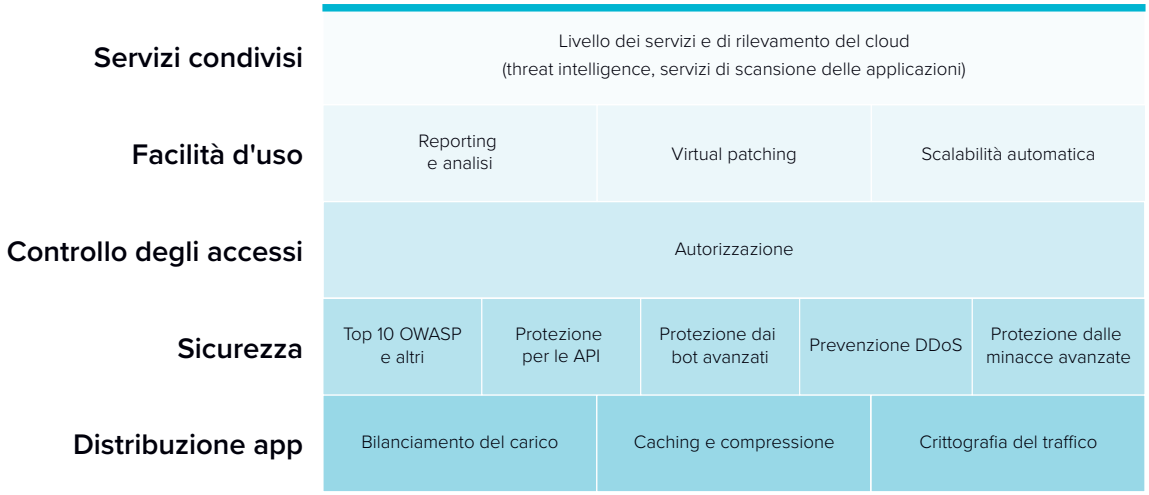
La funzione WAF-as-a-Service di Barracuda offre una procedura guidata iniziale in cinque fasi, semplice da utilizzare, che permette di proteggere le applicazioni in pochi minuti. Gli efficaci modelli già predisposti forniscono protezione completa per le applicazioni di uso più comune. Gli utenti avanzati possono esercitare con facilità un controllo granulare su elementi specifici per impostare criteri di sicurezza personalizzati. Basta aggiungere l'elemento di configurazione che si desidera ottimizzare all'elenco dei componenti della configurazione e regolarli in base alle esigenze specifiche.

Protezione dagli attacchi di nuova generazione

Il servizio è basato su una tecnologia di provata efficacia per le imprese, in grado di difenderle dai principali rischi per la sicurezza indicati nella Top 10 e nel progetto Automated Threats to Web Applications dell'OWASP e da altri rischi, incluse le minacce zero-day. La difesa dai bot avanzati ferma gli attacchi automatizzati, come Web scraping, scalping, clonazione di carte, spam generato da bot e credential-stuffing/furto di account. La protezione DDoS illimitata previene sia gli attacchi DDoS volumetrici che quelli alle applicazioni. Analisi dei rischi e report intuitivi aiutano a produrre la documentazione necessaria per la conformità.

Protezione per le app di nuova generazione

Indipendentemente da dove risieda l'host delle app (on-premise, in cloud, in un contenitore o in ambiente serverless) si possono utilizzare un'API REST e Barracuda Vulnerability Remediation Service, in grado di eseguire la scansione delle vulnerabilità delle applicazioni e risolverle con un solo clic, garantendo in tal modo una sicurezza ininterrotta e ottimizzata, anche se si aggiornano le applicazioni o se ne installano di nuove perché le esigenze aziendali sono cambiate, e senza alcun aggravio amministrativo.



Basato su API e abilitato a DevSecOps

Protegge da tutte queste minacce

- Rischi per la sicurezza delle applicazioni della Top 10 di OWASP
  - Inclusi SQL injection, XSS (Cross-Site Scripting), CSRF (Cross Site Request Forgery), unità esterne XML (XXE, XML External Entities) e altro ancoral
- Bot avanzati
  - Incluse le minacce indicate dall'OWASP nel progetto Automated Threats to Web Applications
- Attacchi di credential-stuffing/furto di account
- Attacchi su API XML e JSON
- Attacchi DDoS volumetrici e alle applicazioni
- Attacchi zero-day
  - Con un potente modello di sicurezza in positivo (positive security) unito a una tecnologia intelligente per le firme per la sicurezza in negativo (negative security)

Protocolli supportati

- HTTP/S/0.9/1.0/1.1/2.0
- WebSocket
- IPv4

Altre funzionalità di sicurezza avanzate

- Protezione basata sull'attendibilità degli indirizzi IP
  - Con geolocalizzazione dell'IP e feed dell'attendibilità basati su sensori nel campo e altri input
- Protezione dal caricamento di file
  - Integrazione con Barracuda Advanced Threat Protection inclusa
- Manomissione dei parametri
- Manipolazione di cookie/form
- Forceful browsing
- Manomissione delle applicazioni
- Convalida dei metadati dei campi dei form
- Cloaking del sito Web
- Controllo della risposta
- Criteri granulari per gli elementi HTML
- Controlli dei limiti dei protocolli
- Database dell'attendibilità degli indirizzi IP di Barracuda
- Fingerprinting euristico
- Test CAPTCHA
- Protezione dal rallentamento del client
- Nodi di uscita ToR
- Elenco dei bloccati di Barracuda
- Protezione DDoS L3-L7 illimitata

Barracuda
Your journey, secured.