CLOUDFLARE

SINTESI DEL PRODOTTO

Cloudflare WAF

Un WAF per la sicurezza delle applicazioni moderne

Problemi di sicurezza delle applicazioni

Le applicazioni sono fondamentali come non mai per le aziende, motivo per cui vengono prese di mira incessantemente dagli aggressori, il che equivale a una superficie d'attacco ampliata.

Le preoccupazioni vanno dal rimanere protetti contro gli exploit zero-day emergenti, al rilevamento dei tentativi di evasione, alla riduzione di sottrazione e uso illecito delle credenziali che porta all'acquisizione dell'account, al rilevamento della perdita di dati, fino alla scansione dei caricamenti di malware nelle applicazioni.

Queste preoccupazioni si uniscono alla necessità di garantire che le protezioni delle applicazioni facciano parte di un approccio di sicurezza più ampio e unificato, che protegga anche le API, arresti i bot e riduca i rischi lato client. Tutto ciò deve avvenire senza gravare sui team con indebiti problemi di gestione.

Cloudflare WAF

Il Web Application Firewall (WAF) di Cloudflare è il fulcro del nostro portafoglio avanzato di sicurezza delle applicazioni che mantiene le applicazioni sicure e produttive. Solo Cloudflare WAF offre una visibilità completa sulla sicurezza, fornisce protezioni a più livelli contro gli attacchi OWASP e gli exploit emergenti, rileva evasioni e nuovi attacchi con il machine learning, blocca l'acquisizione degli account, rileva la perdita di dati e altro ancora, proteggendo le applicazioni ovunque siano ospitate. Le nostre potenti funzionalità di sicurezza delle applicazioni, come la sicurezza API e la mitigazione dei bot, sono totalmente integrate con il nostro WAF, facendo affidamento sullo stesso potente motore di regole, fornito da uno delle migliori connettività cloud al mondo.

Visibilità degli attacchi e onboarding facilitato

Offriamo analisi di sicurezza differenziate per visualizzare tutto il traffico, mitigato o meno. La visibilità immediata nel panorama delle minacce offre un ritorno sull'investimento tangibile, consentendo ai team di comprendere il loro traffico di attacco e le protezioni che dovrebbero creare subito dopo l'onboarding.

Protezioni rapide per gli attacchi emergenti

Con decine di migliaia di vulnerabilità all'anno, il nostro WAF aggiunge rapidamente nuove regole gestite per bloccare gli exploit delle vulnerabilità appena scoperte (giorno 0). Le nostre regole gestite bloccano gli exploit, integrate da WAF Attack Score derivati dal machine learning, per rilevare le evasioni.

Intelligence delle minacce basata su una vasta rete globale

L'efficacia della sicurezza inizia con l'avere i dati migliori e la nostra vasta rete globale utilizza il proxy del 20% di Internet, offrendoci una visione senza precedenti del panorama delle minacce. Questi dati alimentano i modelli di machine learning che affianchiamo ai tradizionali rilevamenti basati sulle firme per trovare e mitigare i tentativi di attacco con elevata precisione.

 | +44 20 3514 6970 | enterprise@cloudflare.com | Cloudflare.com

Problemi di sicurezza delle applicazioni

Cloudflare protegge in modo più efficace.

Forniamo una sicurezza WAF più efficace con protezioni a più livelli:

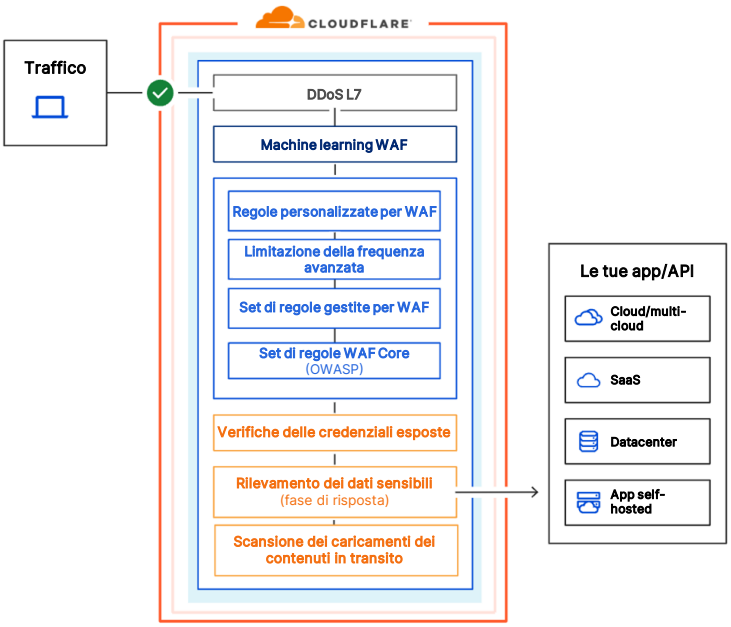
- Analisi della sicurezza
- Più set di regole gestiti
- Regole personalizzate
- Rilevamenti basati sul machine learning
- Rilevamento dei dati sensibili
- Controlli di credenziali sottratte
- Limitazione della frequenza avanzata
- Scansione anti-malware dei caricamenti

Cloudflare risponde più velocemente.

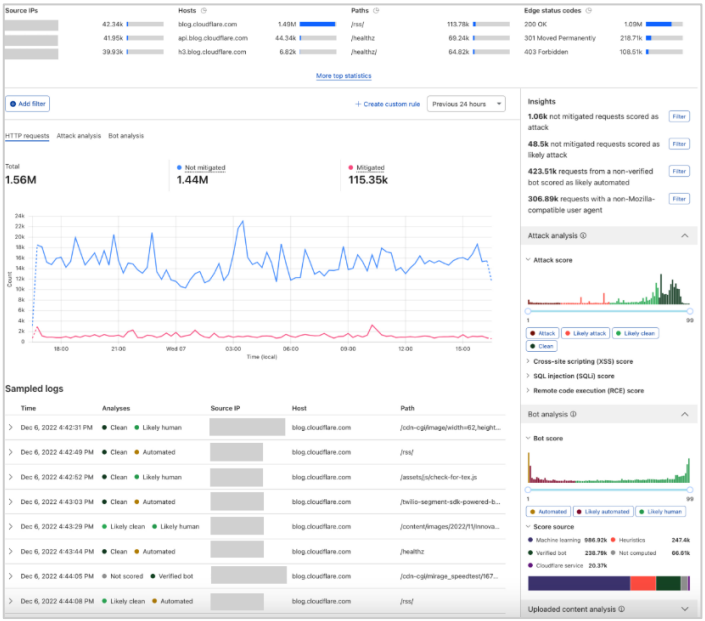
Proteggiamo più velocemente dagli exploit. Per le principali vulnerabilità come HTTP/2 Rapid Reset, Log4j e molte altre, avevamo più regole gestite in atto un giorno lavorativo più velocemente rispetto ad altri fornitori WAF .

Cloudflare integra completamente la sicurezza delle applicazioni.

Il nostro WAF è completamente integrato con il resto del nostro portafoglio di sicurezza delle applicazioni, inclusi API Gateway e gestione dei bot, il tutto fornito in un unico passaggio dalla connettività cloud di Cloudflare.



Analisi della sicurezza WAF



Un WAF per la sicurezza aziendale

Integrato con SIEM, pronto per SOC

Con le API Cloudflare e le integrazioni dei registri con dati non elaborati, è facile integrarsi con il tuo SIEM o potenziare il tuo centro operativo di sicurezza (SOC) con l'intelligence fornita da Cloudflare.

DevSecOps facilitato

La nostra integrazione Terraform pronta all'uso fa sì che l'incorporazione della sicurezza delle applicazioni in DevOps si avvicini a una seconda natura.

Supportato da Cloudforce One

La sicurezza delle applicazioni di Cloudflare riceve l'intelligence delle minacce da Cloudforce One, il nostro team operativo sulle minacce, che blocca le minacce tramite nuovi rilevamenti basati su informazioni emergenti e TTP.

Sicurezza delle applicazioni Web	
Protezioni a livelli da più set di regole WAF	Blocca i payload dannosi in qualsiasi componente della richiesta con più set di regole: 1. Regole gestite da Cloudflare 2. Set di regole principali OWASP 3. Set di regole personalizzate per bloccare qualsiasi attacco. Nuove regole gestite testate su grandi quantità di traffico per garantire il minor numero di falsi positivi.
Regole aggiornate per le protezioni zero-day	Regole aggiornate continuamente dai team di sicurezza di Cloudflare per la protezione da nuovi attacchi e exploit di vulnerabilità zero-day prima che siano disponibili patch o aggiornamenti.
Rilevamenti basati sul machine learning	Blocca i tentativi di aggiramento con modelli di machine learning per integrare i set di regole a più livelli. Per le regole sono disponibili quattro diversi punteggi di attacco: WAF Attack Score complessivo, punteggio di attacco XSS, punteggio di attacco SQL e punteggio di attacco RCE.
Set di regole specifiche della piattaforma per le principali piattaforme CMS e e-commerce	Ricevi protezione immediata senza costi aggiuntivi per piattaforme come WordPress, Joomla, Plone, Drupal, Magneto, IIS ecc.
Configurazione delle regole personalizzate	Crea un modello di sicurezza positivo o negativo utilizzando le seguenti azioni: BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES durante la distribuzione di regole o set di regole.
Limitazione della frequenza avanzata	Blocca gli abusi, gli attacchi DDoS e i tentativi di forza bruta mirati ad applicazioni e API limitando la frequenza dei singoli IP o per intestazione (ad esempio, chiave, cookie, token), ASN o paese.
Rilevamento dei dati sensibili	Rileva le risposte contenenti dati sensibili come informazioni di identificazione personale (PII), informazioni finanziarie, numeri di carte di credito o segreti come chiavi API.
Verifiche delle credenziali esposte	Rileva gli attacchi di sottrazione e uso illecito delle credenziali con credenziali sottratte prima che venga assunto il controllo degli account degli utenti finali.
Scansioni di caricamento dei contenuti	WAF Content Scanning eseguirà la scansione dei file caricati alla ricerca di malware e puoi combinare i suoi segnali con altri parametri della richiesta creando regole personalizzate.
SSL/TLS	Scarica e configura completamente il traffico SSL per la tua applicazione.
Meno falsi positivi	Nuove regole testate su grandi quantità di traffico per garantire il minor numero di falsi positivi.
Supporto gRPC e Websocket	Proxy e traffico sicuro per gli endpoint gRPC e Websocket.
Pagine di blocco personalizzabili	Personalizza le pagine di blocco con i dettagli appropriati per i visitatori.
Integrazione completa con la più ampia suite di prodotti Cloudflare	Migliora le prestazioni delle applicazioni, il traffico del percorso geografico e sfrutta l'edge computing.

Visibilità, segnalazione e programmabilità	
Analisi della sicurezza	Visualizzazione di tutti i potenziali attacchi, valutati dal machine learning.
Registrazione in tempo reale e accesso ai file di log non elaborati	Ottieni visibilità per aiutarti a mettere a punto il WAF, conduci un'analisi approfondita che copre tutte le richieste WAF.
Registrazione dei payload	Registra e crittografa i payload dannosi per l'analisi degli incidenti.
Integrazioni SIEM	Inserisci o estrai i log direttamente nei tuoi SIEM esistenti.
Integrazione Terraform	Incorpora la sicurezza delle applicazioni nei flussi di lavoro CI/CD.
Gestione	
Gestione con un'unica console	Gestione semplificata con un'unica console per distribuire e gestire la sicurezza e le prestazioni globali delle applicazioni.
Gestione a livello di account	Risparmia tempo sulla gestione WAF tramite un'unica configurazione WAF a livello di account per tutti i domini.
Alta disponibilità con gli SLA	Garanzia del 100% di uptime, comprese sanzioni pecuniarie in caso di violazione degli SLA.
Nessun hardware, software o messa a punto richiesta	Distribuisci con una semplice modifica nel DNS.
Certificazione PCI	Cloudflare possiede la certificazione di provider di servizi di Livello 1.
Autorizzato da FedRAMP	La nostra suite Cloudflare for Government, che include la sicurezza per le applicazioni, è autorizzata da FedRAMP.

Ti va di saperne di più? Registrati alla nostra serie di demo sulla sicurezza delle applicazioni.

 | +44 20 3514 6970 | enterprise@cloudflare.com | Cloudflare.com