Un WAF per la sicurezza delle applicazioni moderne

Le aziende si affidano ad applicazioni e API per la crescita e, e con la sicurezza delle applicazioni Cloudflare di prim'ordine, l'espansione delle superfici di attacco e nuovi attacchi non sono mai d'intralcio.

Cloudflare Web Application Firewall (WAF) è la punta di diamante del nostro portafoglio avanzato di sicurezza delle applicazioni che mantiene le applicazioni e le API sicure e produttive, impedisce gli attacchi DDoS, tiene a bada i bot, rileva anomalie e payload dannosi, il tutto monitorando gli attacchi della supply chain del browser.

Le nostre potenti funzionalità di sicurezza delle applicazioni sono integrate con il resto del nostro portafoglio di prestazioni delle applicazioni leader, tutte fornite dalla piattaforma cloud globale più connessa al mondo.

Web Application Firewall di Cloudflare

Il nostro WAF viene fornito dalla nostra rete perimetrale globale per una sicurezza di livello aziendale, che copre oltre 250 città in più di 100 paesi per prestazioni e affidabilità incredibili, in grado di scalare illimitate e istantanee.

Potenti protezioni Cloudflare

Cloudflare offre potenti set di regole che bloccano le minacce, inclusi gli zero-day scoperti di recente, oltre a bypass e variazioni di attacco utilizzando il machine learning. Inoltre, con le regole personalizzate granulari, puoi configurare il WAF per la protezione da qualsiasi minaccia o adottare criteri di sicurezza specifici per l'azienda.

Maggiore sicurezza grazie all'intelligence globale

La nostra intelligence sulle minacce è costantemente rafforzata dalle informazioni acquisite dalla nostra rete globale che elabora 2 trilioni di richieste giornaliere, assicurando che il nostro WAF mantenga le organizzazioni più sicure contro le minacce emergenti.

Implementazione rapida e gestione facilitata

La protezione globale WAF è attiva con pochi clic. Niente da distribuire, nessuna formazione lunga settimane o spese per servizi professionali, hai un unico pannello per gestire tutto.

Protezione globale in pochi secondi

Le minacce si muovono velocemente ma le nostre protezioni tengono il passo. Per una protezione istantanea, le nuove regole sono attive in pochi secondi , a differenza di altri WAF, che richiedono 45 minuti o più per attivare la protezione.

Sicurezza delle applicazioni dal perimetro di Internet

Le organizzazioni ottengono una posizione di sicurezza delle applicazioni più efficace, indipendentemente dal fatto che le app siano on-premise o nel cloud, grazie alla rete globale Cloudflare come perimetro di sicurezza aziendale, che blocca 86 miliardi di minacce al giorno.

La protezione più veloce e precisa

Trova sempre il giusto compromesso tra sicurezza e business con protezioni precise, testate contro grandi quantità di traffico, che non bloccano mai il business. La nostra rete garantisce ai clienti una protezione fino a 10 volte più veloce rispetto alla concorrenza.

Vasta capacità integrata

Nessuna base di codice di acquisizione alla buona piuttosto, la sicurezza integrata affina costantemente la sua capacità di fermare le minacce. Prestazioni come CDN, DNS, bilanciamento del carico e accelerazione del traffico sono tutte integrate.

Un unico potente pannello di controllo

Gestisci facilmente la sicurezza e aggiungi rapidamente nuove funzionalità con la nostra console unica. Nessuna interfaccia o sintassi delle regole eccessivamente complesse. Solo una sicurezza potente dalla nostra console unica e intuitiva.

Stato di sicurezza completo

Le nostre funzionalità di sicurezza offrono sempre funzionalità complete, pronte per l'azienda e convenienti. Non ti dissangueremo mai con offerte di base limitate che richiedono componenti aggiuntivi costosi o integrazioni di mercato di terze parti per un solido stato di sicurezza.

Sicurezza delle applicazioni aziendali

Innovazione della sicurezza L7

Includiamo protezioni avanzate contro l'utilizzo di credenziali esposte e avvisi su Javascript di terze parti potenzialmente infetti nelle tue applicazioni che potrebbero eseguire attacchi basati sulla supply chain.

Integrato con SIEM, pronto per SOC

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

DevSecOps facilitato

Sei pronto per lo shift left della sicurezza? Noi lo siamo. La nostra integrazione Terraform pronta all'uso fa sì che l'incorporazione della sicurezza delle applicazioni in DevOps si avvicini a una seconda natura.

Leadership Cloudflare

Le organizzazioni ottengono una posizione di sicurezza delle applicazioni più efficace con la rete globale Cloudflare come perimetro di sicurezza aziendale. Il portafoglio di sicurezza delle applicazioni Cloudflare ha ricevuto numerosi riconoscimenti per la sua forza e ampiezza. Gartner ha nominato il WAF Cloudflare Scelta del cliente 2021. Frost & Sullivan ha riconosciuto Cloudflare come leader dell'innovazione nella protezione Web olistica globale, mentre IDC e Forrester hanno nominato l'azienda leader DDoS.

Funzionalità principali	Vantaggi
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 • Regole gestite da Cloudflare • Set di regole di terze parti (Top ten OWASP) • Set di regole personalizzate per fermare qualsiasi attacco
WAF ML: rilevamenti basati sul machine learning	Arresta bypass, variazioni di attacco e anomalie sfruttando i punteggi di attacco generati da ML nelle regole personalizzate WAF.
Regole aggiornate per le protezioni zero-day	Regole continuamente aggiornate dal team di sicurezza di Cloudflare o protezione contro nuovi attacchi e vulnerabilità zero-day prima che siano disponibili patch o aggiornamenti.
Set di regole specifiche della piattaforma per le principali piattaforme CMS ed eCommerce	Ricevi protezione immediata senza costi aggiuntivi per piattaforme come WordPress, Joomla, Plone, Drupal, Magneto, IIS, ecc.
Configurazione delle regole personalizzate	Scegli tra BLOCK, LOG, CHALLENGE, CAPTCHA CHALLENGE, RATE LIMIT e altre opzioni durante la distribuzione di regole o set di regole.
Limitazione della frequenza avanzata	Ferma 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, ASN o paese.
Database reputazioni IP	Blocca le connessioni da IP dannosi con intelligence in tempo reale su oltre 1 miliardo di IP univoci.
Prevenzione contro la perdita dei dati	Blocca le risposte contenenti dati sensibili come informazioni di identificazione personale, informazioni finanziarie, numeri di carte di credito o segreti come chiavi API.
Verifiche delle credenziali esposte	Rileva gli attacchi di forza bruta con le credenziali rubate prima che gli account degli utenti finali vengano presi in consegna.
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.

FUNZIONALITÀ DI SICUREZZA DELLE APPLICAZIONI	
Mitigazione dei bot	Protezione contro i bot con opzioni sofisticate di protezione a più livelli, visibilità e problemi.
Mitigazione DDoS	Consente una protezione completa contro gli attacchi DDoS.
Sicurezza lato client	Rileva e blocca gli attacchi alla supply chain basati su browser.
Protezione API	Proteggi il traffico API come definito dagli schemi o rilevato dai modelli di machine learning di Cloudflare.
REPORTING E PROGRAMMABILITÀ	
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 del 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	
Singola console di gestione	Gestione semplificata con un'unica console per distribuire e gestire la sicurezza e le prestazioni globali delle applicazioni.
Alta disponibilità basata sugli SLA dell'offerta di servizi	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.