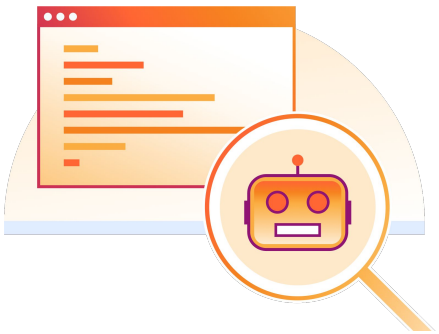
Cloudflare Bot Management

Blocca i bot dannosi e gestisci i bot IA senza bisogno di CAPTCHA.



I bot si nascondono nel tuo traffico. I bot dannosi compromettono i ricavi e l'esperienza utente.

Il **30%** del traffico delle applicazioni su Internet è traffico automatizzato[1]. Le difese tradizionali, come l'euristica basata sulla posizione geografica e l'IP, nonché i CAPTCHA, vengono facilmente aggirate dai bot moderni. Ciò provoca una grossa frustrazione per gli utenti reali.

Grazie alla visibilità su **circa il 20%** del Web, nessun altro provider controlla più crawler IA e bot di ricerca di Cloudflare[2].

Cloudflare Bot Management aiuta le organizzazioni a gestire i crawler IA e il traffico bot verso app Web e mobili senza CAPTCHA. Consenti l'accesso alle app a bot verificati e crawler IA conformi, contestando e bloccando al contempo i bot IA non conformi e quelli dannosi. Si tratta di una funzionalità chiave nel nostro portfolio per la sicurezza delle applicazioni.

Vantaggi del prodotto

- Protezione da frodi, perdite finanziarie e danni all'immagine del marchio
- Offri esperienze migliori per app Web e per dispositivi mobili
- Ottieni l'indipendenza dai crawler IA e dai bot di ricerca indesiderati

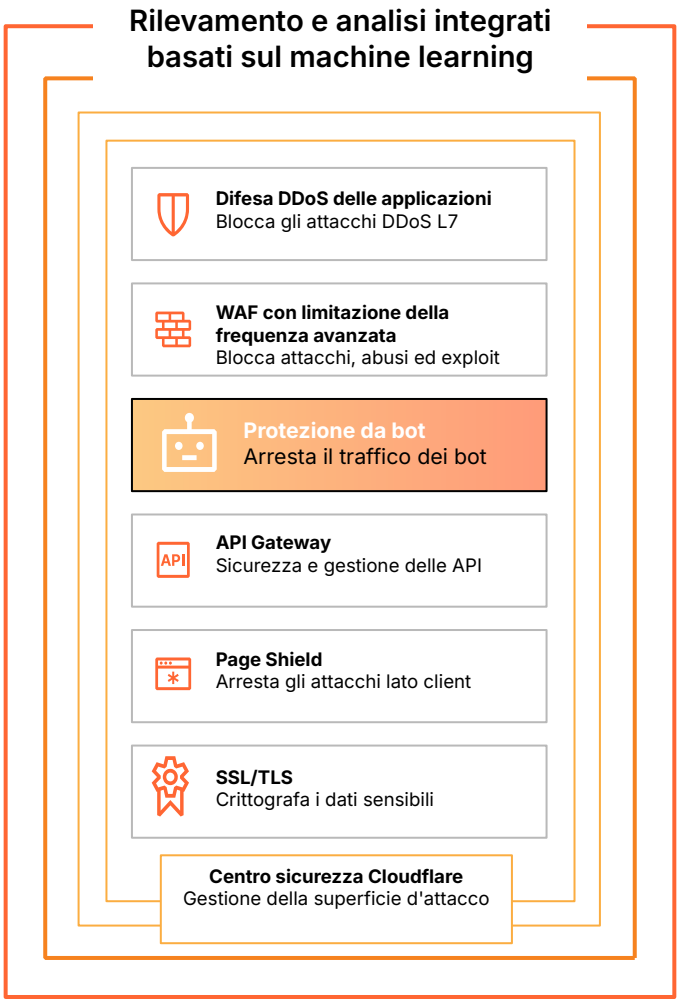


Figura 1: Cloudflare Bot Management integrato nel nostro portafoglio di sicurezza delle applicazioni

Fonti

1. Dati di Cloudflare Radar, 2024
2. W3techs, Usage statistics and market shares of reverse proxy services, 2025

Come funziona Cloudflare Bot Management

Cloudflare combina il rilevamento a più livelli da machine learning globale e specifico per app, JavaScript lato client, dispositivi mobili ed euristica in un unico punteggio bot che. viene assegnato a ogni richiesta HTTP. Un punteggio dei bot indica la probabilità che tale richiesta provenga da un bot. Questo punteggio bot viene utilizzato per le risposte standard, come blocco o autorizzazione, e per i criteri di risposta personalizzati tramite altri prodotti Cloudflare. Le analisi dei bot, inclusi il punteggio dei bot, i metadati delle richieste HTTP e altro, sono disponibili nell'interfaccia utente del dashboard di Cloudflare o tramite l'API di Cloudflare negli strumenti di terze parti.

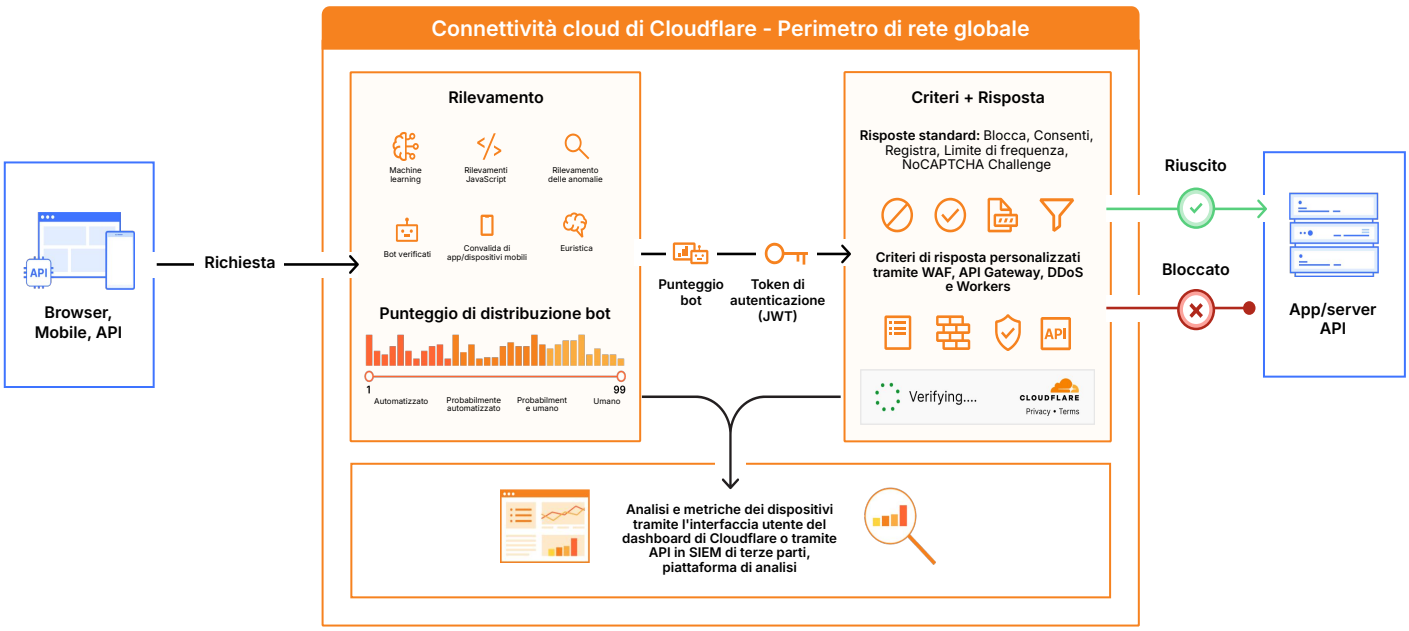


Figura 2: Percorso di richiesta di esempio tramite Cloudflare Bot Management

Funzionalità principali di Cloudflare Bot Management

Acquisizione e abuso di account

Proteggiti dagli attacchi zero-day con modelli basati su ML in grado di rilevare le vulnerabilità più rapidamente della divulgazione al pubblico. Difenditi dagli attacchi DDoS da record, proteggi i dati sensibili, riduci i rischi lato client e monitora la supply chain del software della tua applicazione Web.

Difesa da bot e frodi

Proteggi i tuoi utenti dall'acquisizione dell'account e blocca i bot dannosi che compromettono l'esperienza dell'utente finale. Blocca botnet dannose, sottrazione e uso illecito di credenziali e carte di credito, scraping di contenuti e accaparramento delle scorte combinando modelli ML con intelligence delle minacce e informazioni su client e rete.

Gestione di bot e crawler IA

Esercita un controllo più rigoroso sui contenuti e sui costi bloccando i crawler IA, addebitando loro i costi o intrappolandoli in loop senza fine. Ottieni visibilità sui modelli di richiesta e sulla conformità con le direttive robots.txt. Disponibile per tutti i clienti di Cloudflare.

Funzionalità chiave	
Motori di rilevamento	
Machine learning	Il nostro modello di machine learning globale è addestrato sull'intero traffico di rete globale di Cloudflare, che instrada miliardi di richieste ogni giorno, per identificare il traffico automatizzato e umano. Tutto ciò è incluso nel nostro punteggio bot complessivo. I clienti vengono aggiornati automaticamente all'ultimo modello.
Rilevamento delle anomalie	I nostri modelli di anomalia dei comportamenti basati sull'apprendimento non supervisionato definiscono i modelli di traffico specifici dell'applicazione e calibrano le soglie delle regole per identificare comportamenti anomali dei bot in base alle variazioni dei modelli di traffico dei clienti nel tempo. Tutto ciò è incluso nel nostro punteggio bot complessivo.
Euristica	Per identificare i bot utilizziamo modelli noti di comportamento dannoso dei bot, ricavati dal traffico precedente. Aggiorniamo regolarmente la nostra euristica per tutti i clienti. Tutto ciò è incluso nel nostro punteggio bot complessivo.
Bot verificati e bot IA	La nostra directory dei bot identifica gli ID di rilevamento dei bot noti che svolgono funzioni legittime e operano in modo trasparente come bot verificati, come prescritto dalla politica sui bot verificati di Cloudflare. Abbiamo una categoria separata per i bot IA conosciuti, che potrebbero rispettare o meno il file robots.txt e nascondere il loro comportamento dalle tue app.
Rilevamento JavaScript	Il modulo di rilevamento JavaScript identifica i browser headless e altre impronte digitali dannose tramite una JavaScript injection leggera e invisibile sul lato client di qualsiasi richiesta. Rispettiamo standard di privacy molto rigidi e non raccogliamo le informazioni di identificazione personale (PII) durante il processo.
Punteggio bot	Utilizza il punteggio bot per scrivere meno regole per catturare la maggior parte dei bot invece di scrivere una regola per ogni ID o tipo di bot. Il punteggio bot utilizza l'intelligence dei nostri motori di rilevamento per produrre un punteggio da 1 a 99 che indica la probabilità che una richiesta provenga da un bot. Un punteggio pari a 1 si riferisce a richieste sicuramente automatizzate e un punteggio di 99 si riferisce a richieste sicuramente umane.
Convalida dei dispositivi tramite SDK di dispositivi mobili	Questi SDK per tutte le principali piattaforme di app mobili, tra cui Android, iOS, React Native, Unity e altre, confermano l'integrità delle app, rilevano ambienti non sicuri e autenticano il traffico API (con token di crittografia forniti autonomamente o approvati da Cloudflare).
Criteri e risposte	
Risposte standard	Configura le azioni Blocco, Consenti, Registra, Limite di frequenza o una serie di sfide intuitive come risposta al traffico bot identificato dai nostri motori di rilevamento.
Criteri di risposta personalizzati	Incorpora i segnali di gestione dei bot nei criteri di altri prodotti Cloudflare, come Cloudflare WAF e DDoS, e definisci azioni personalizzate tramite Workers.
Analisi	
Dashboard di Cloudflare	Esamina l'attività dei bot fino a 30 giorni e filtra in base al punteggio del bot e ad altri filtri relativi a bot, traffico bot e richieste. Il ciclo di feedback dei bot permette ai clienti di segnalare a Cloudflare eventuali falsi positivi o falsi negativi per ulteriori accertamenti.
Strumenti di terze parti (SIEM, data lake, strumenti di analisi, ecc.)	Analizza i segnali di gestione dei bot in tutte le tue app in un unico dashboard tramite sicurezza Cloudflare Analytics, esplora dati di log aggiuntivi in Log Explorer e combina dati di terze parti con dati Cloudflare in SIEM o piattaforme di analisi di terze parti tramite Log Push.

Vuoi saperne di più? Registrati alla nostra serie dimostrativa sulla sicurezza delle app.