CLOUDFLARE

KURZDARSTELLUNG

Bot-Management von Cloudflare

Schadbots stoppen und KI-Bots ohne CAPTCHA abfertigen

Im Datenverkehr verborgene Schadbots beeinträchtigen Umsatz und Nutzererlebnis

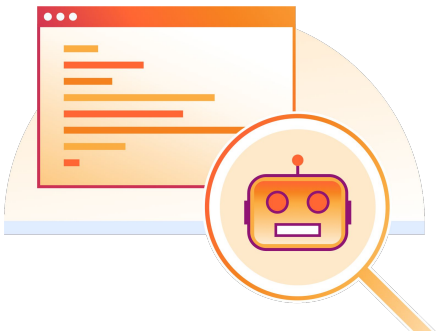
30 % des Anwendungstraffics im Internet gehen auf Bots zurück.[1] Herkömmliche Abwehrmaßnahmen wie Standort- und IP-basierte Heuristiken und CAPTCHA können von modernen Bots problemlos umgangen werden. Gleichzeitig sind sie für echte Nutzer ein großes Ärgernis.

Bei Cloudflare haben wir Einblick in **rund 20 %** des Internets, wodurch wir mehr KI-Crawler und Such-Bots identifizieren und nachverfolgen können als alle anderen Anbieter.[2]

Das **Bot-Management von Cloudflare** hilft bei der Handhabung von KI-Crawlern und Bot-Traffic für Web- und Mobilgeräte-Anwendungen ohne CAPTCHA. Während verifizierten Bots und den Vorgaben entsprechenden KI-Crawlern Zugriff auf Applikationen erhalten, werden unerwünschte KI- und Schadbots erkannt und gestoppt. Es handelt sich um eine wichtige Funktion unserer Produkte für Anwendungssicherheit.

Produktvorteile

- Schutz vor Betrug, finanziellen Verlusten und Imageschäden
- Verbesserung der Nutzererfahrung für Web- und Mobilgeräte-Anwendungen
- Unabhängigkeit von unerwünschten KI-Crawlern und Such-Bots



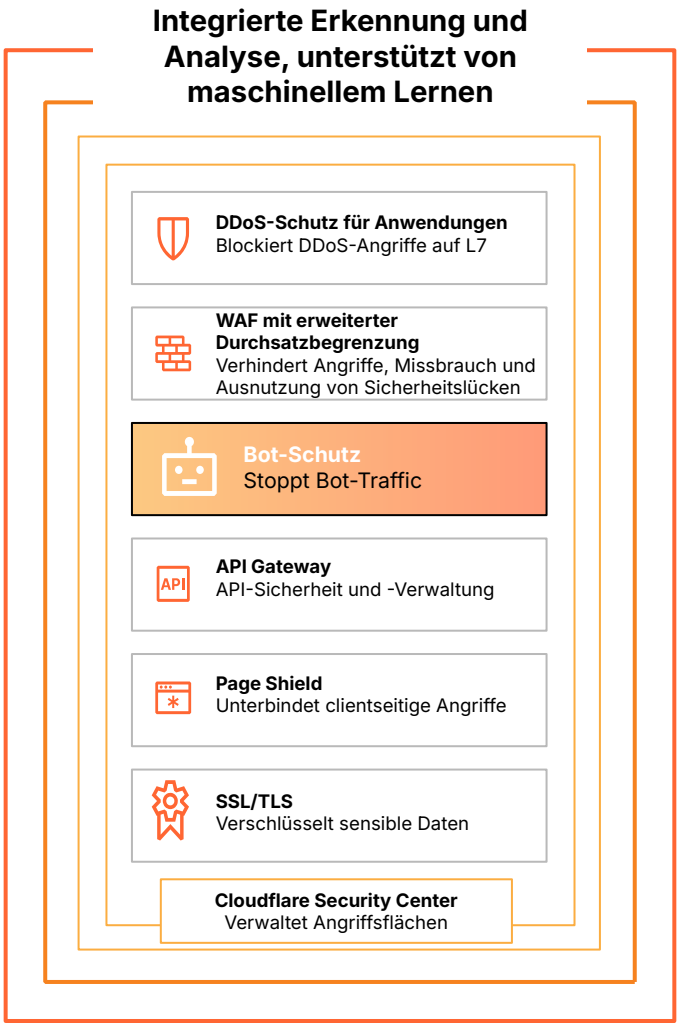


Abbildung 1: Das Bot-Management von Cloudflare ist in unsere Produkte für Anwendungssicherheit integriert

Quellen

1. Cloudflare Radar-Daten, 2024
2. W3techs, Nutzungsstatistiken und Marktanteile von Reverse-Proxy-Diensten, 2025

So funktioniert das Bot-Management von Cloudflare

Cloudflare führt mehrstufige Bedrohungserkennung mit Erkenntnissen aus globalem und anwendungsspezifischem Machine Learning, clientseitigem JavaScript, Mobilgeräten und Heuristiken in einem einzigen Bot-Score zusammen, der für jede HTTP-Anfrage erstellt wird. Dieser gibt die Wahrscheinlichkeit an, mit der eine Anfrage von einem Bot stammt. Er wird für Standardreaktionen wie das Blockieren oder Zulassen von Anfragen sowie für nutzerdefinierte Reaktionsrichtlinien in anderen Cloudflare-Produkten verwendet. Bot-Analysedaten, einschließlich Bot-Score und HTTP-Anfrage-Metadaten, sind über das Cloudflare-Dashboard oder über die Cloudflare-API in externen Tools verfügbar.

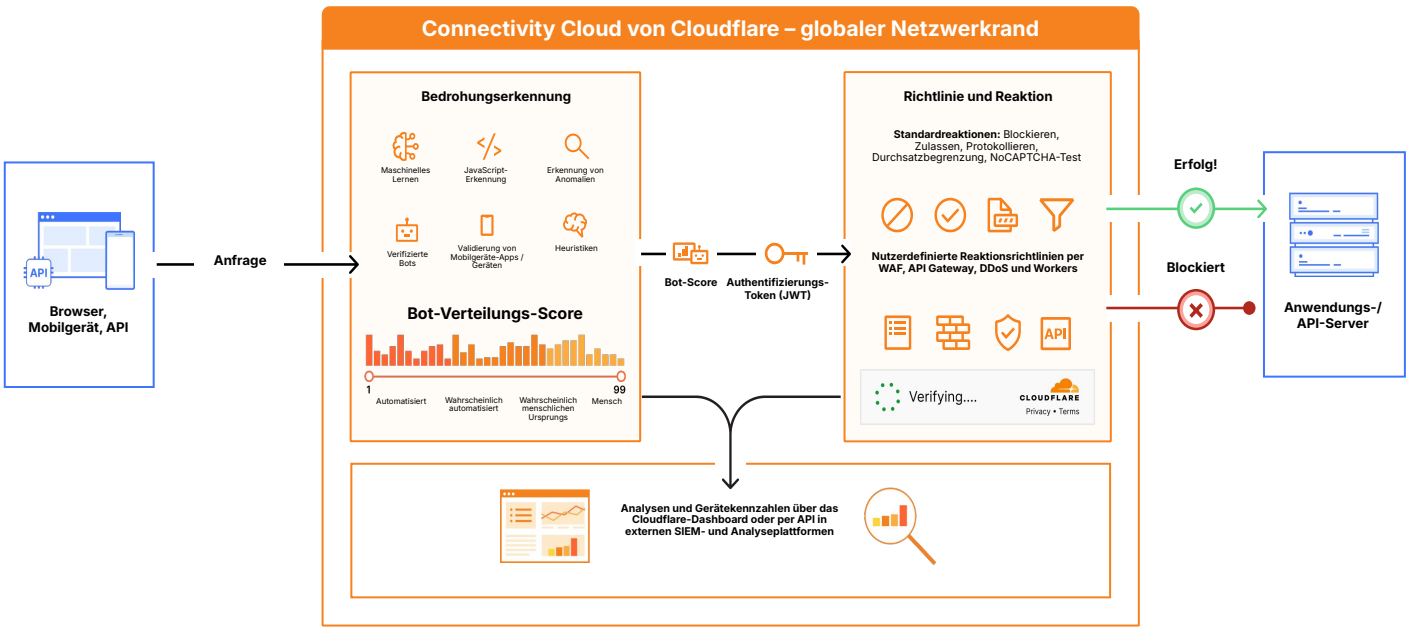


Abbildung 2: Beispiel für einen Anfragepfad innerhalb des Bot-Managements von Cloudflare

Wichtige Funktionen des Bot-Managements von Cloudflare

Kontoübernahmen und Missbrauch

Machine Learning-gestützte Modelle spüren Sicherheitslücken noch vor ihrer öffentlichen Bekanntgabe auf und schützen so vor Zero-Day-Angriffen. Sie können DDoS-Rekordangriffe abwehren, vertrauliche Daten schützen, clientseitige Risiken verringern und die Software-Lieferkette Ihrer Webanwendung im Auge behalten.

Abwehr von Bot-Angriffen und Betrug

Anwender werden vor Kontoübernahmen bewahrt und vor Schadbots geschützt, die das Endnutzererlebnis beeinträchtigen. Machine Learning-Modelle werden mit Informationen, unter anderem Bedrohungsdaten, von Clients und Netzwerken gefüttert. So wird bösartigen Botnetzen, Credential Stuffing (auch in Bezug auf Kreditkarten), Content Scraping und Inventory Hoarding Einhalt geboten.

Abfertigung von KI-Crawlern und Bots

KI-Crawler können blockiert, mit Gebühren belegt oder in Endlosschleifen gehalten werden, was eine größere Kontrolle über Inhalte und Kosten ermöglicht. Sie erhalten einen Überblick über Anfrage-Muster und die Einhaltung Ihrer robots.txt-Vorgaben. Diese Funktionen stehen allen Cloudflare-Kunden zur Verfügung.

Wichtigste Funktionen	
Engines zur Bedrohungserkennung	
Maschinelles Lernen	Unser Machine-Learning-Modell wird mit dem gesamten Traffic des globalen Netzwerks von Cloudflare trainiert, das täglich für Milliarden von Anfragen als Proxy dient. Dadurch ist es in der Lage, zwischen automatisiertem und auf Menschen zurückgehenden Datenverkehr zu unterscheiden. Dies fließt in unseren Bot-Gesamtscore ein. Die Aktualisierung auf das neueste Modell erfolgt für Kunden automatisch.
Erkennung von Anomalien	Unsere unüberwachten, lernfähigen Modelle zur Erkennung von Verhaltensanomalien ziehen anwendungsspezifische Datenverkehrsmuster als Referenz heran und kalibrieren Regelschwellenwerte, um ungewöhnliches Verhalten von Bots zu registrieren, da sich die Traffic-Muster der Kunden mit der Zeit verändern. Dies fließt in unseren Bot-Gesamtscore ein.
Heuristiken	Wir nutzen zur Einstufung von Bots bekannte Verhaltensmuster von Schadbots aus früherem Traffic. Unsere Heuristiken werden für alle Kunden regelmäßig auf den neuesten Stand gebracht. Dies fließt in unseren Bot-Gesamtscore ein.
Verifizierte und KI-gestützte Bots	Mithilfe unseres Bot-Verzeichnisses können wir die ID bekannter Bots zuordnen, die gemäß der einschlägigen Cloudflare-Richtlinien zu legitimen Zwecken und transparent als verifizierte Bots eingesetzt werden. Wir verfügen über eine separate Kategorie für bekannte KI-Bots, ob diese nun die robots.txt beachten oder nicht, die ihr Verhalten vor Ihren Anwendungen verbergen.
JavaScript-Erkennung	Das JavaScript-Erkennungsmodul identifiziert Headless-Browser und andere bösartige Fingerabdrücke mittels einer schlanken, unsichtbaren JavaScript-Injection auf Clientseite jeder Anfrage. Wir halten dabei sehr strenge Datenschutzstandards ein und erfassen während dieses Vorgangs keine personenbezogenen Daten.
Bot-Score	Bei Verwendung des Bot-Scores werden die meisten Bots erkannt, ohne dass für jede Bot-ID oder jeden Bot-Typ eine eigene Regel erstellt werden muss. Im Rahmen der Bot-Score-Funktion wird anhand von Informationen aus unseren Erkennungs-Engines ein Wert zwischen 1 und 99 generiert. Daran lässt sich die Wahrscheinlichkeit dafür ablesen, dass eine Anfrage von einem Bot stammt, wobei ein Wert von 1 eine eindeutig automatisierte Anfrage und ein Wert von 99 eine unzweifelhaft von einem Menschen stammende Anfrage anzeigt.
Gerätevalidierung per Mobilgeräte-SDK	Diese SDK für alle wichtigen Plattformen für Mobilgeräte-App, darunter Android, iOS, React Native und Unity, validieren die App-Integrität, erkennen unsichere Umgebungen und authentifizieren den API-Datenverkehr (mit selbst bereitgestellten oder von Cloudflare genehmigten kryptografischen Token).
Richtlinie und Reaktion	
Standardreaktion	Für den von unseren Erkennungs-Engines als solchen identifizierten Bot-Traffic können die Maßnahmen Blockieren, Zulassen, Protokollieren und Durchsatzbegrenzung oder diverse nutzerfreundliche Tests eingerichtet werden.
Nutzerdefinierte Richtlinien für Reaktionen	Bot-Management-Hinweise können in Richtlinien anderer Cloudflare-Produkte wie unserer WAF oder DDoS-Abwehr integriert werden. Darüber hinaus lassen sich über Workers nutzerdefinierte Aktionen festlegen.
Analysedaten	
Cloudflare-Dashboard	Hier sind die Bot-Aktivitäten der letzten 30 Tage einsehbar. Außerdem besteht die Möglichkeit, nach Bot-Score und anderen Bot-, Traffic- und Anfragemerkmalen zu filtern. Die Bot-Feedbackschleife erlaubt es Kunden, Positiv- oder Negativ-Falschmeldungen für weitere Nachforschungen bei Cloudflare zu melden.
Externe Tools (SIEM, Data Lake, Analysewerkzeuge usw.)	Bot-Management-Hinweise können für alle Anwendungen innerhalb eines einzigen Dashboards über Security Analytics von Cloudflare analysiert werden. Zudem lassen sich zusätzliche Protokolldaten im Log Explorer untersuchen und Daten von Drittanbietern in externen SIEM- oder Analyseplattformen per Log Push mit denen von Cloudflare kombinieren.

Haben wir Sie neugierig gemacht? Dann registrieren Sie sich für unsere Demo-Reihe zu Anwendungssicherheit.