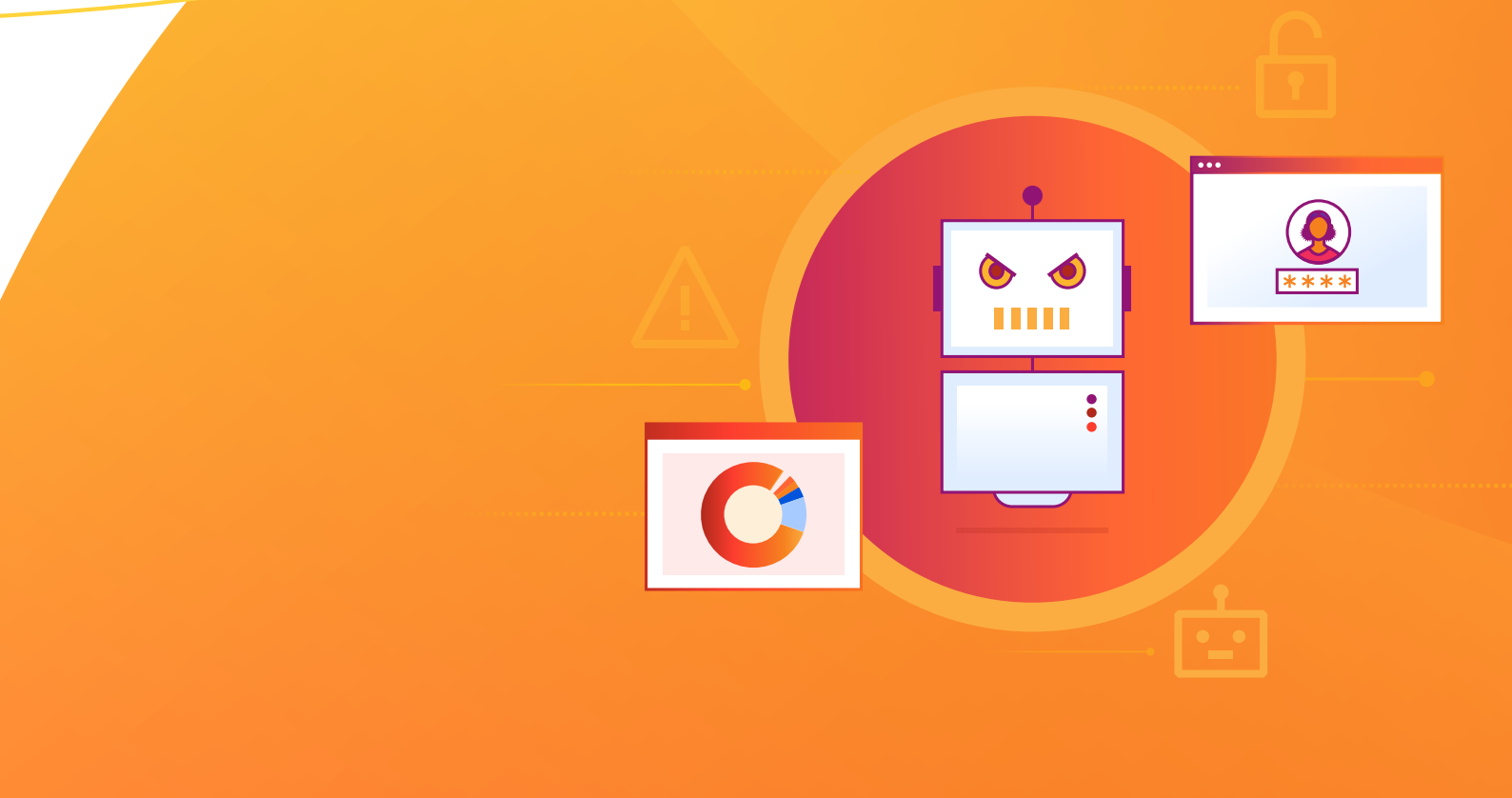
CLOUDFLARE

WHITEPAPER

Der Leitfaden zu böswilligen Bots: Frühwarnzeichen und Gegenmaßnahmen



Inhalt

Einleitung

Bots machen heute etwa 30 % des Online-Traffics aus, und viele dieser Bots sind darauf aus, Organisationen wie Ihre zu schädigen, wobei schätzungsweise 93 % dieses Bot-Traffics nicht verifiziert und potenziell bösartig sind. Die Verbreitung von Content- und Price-Scraping, Kontoübernahme, Stuffing von Anmeldedaten und Kreditkartendaten, Inventory Hoarding und Botnet-gesteuerten Distributed-Denial-of-Service (DDoS-Angriffen) deutet darauf hin, dass bösartige Bot-Akteure von Jahr zu Jahr komplexer und raffinierter werden.

Darüber hinaus sind herkömmliche Anti-Bot-Maßnahmen wie Standortblockierung, IP-Adressblockierung und traditionelle CAPTCHAs heutzutage unwirksam. Tatsächlich sind CAPTCHAs für Bots leichter zu lösen als für Menschen.[1]

Deshalb gibt es kein Patentrezept, um alle Bots abzuwehren und Ihre Benutzer und Ihre Marke zu schützen. Die einzige Lösung: Nach einer Vielzahl von verräterischen Warnzeichen für Bots Ausschau halten und auf jedes einzelne reagieren. Dazu müssen Daten gesammelt und zielgerichtete Gegenmaßnahmen, Mustererkennung, prädiktive Analysen und andere ergänzende Strategien eingesetzt werden.

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

Warnzeichen für ein Bot-Problem

Durch das Überwachen einer Reihe potenzieller Indikatoren haben Sie sehr gute Chancen, schädliche Bots zu erkennen, bevor diese ernsthaften Schaden anrichten können. Auf folgende Anzeichen sollten Sie achten:

Höhere Infrastrukturkosten bei gleichbleibendem Geschäftsvolumen

Der gesamte Traffic Ihrer Website ist mit Kosten verbunden. Unabhängig davon, wer oder was auf Ihre Inhalte zugreift, müssen Sie die Kosten für Speicherung und Computing tragen. Aber schädliche Bots können Ihre Traffic-bezogenen Kosten erhöhen, ohne Ihrem Unternehmen Einnahmen zu verschaffen. Vertrauenswürdige Bots werden von Suchmaschinen eingesetzt, um Inhalte auf Ihrer Website zu indexieren, wodurch sich Ihr SEO-Ranking verbessert. Schädliche Bots dagegen verursachen jedes Jahr erhebliche zusätzliche Bandbreitenkosten.

Ungewöhnliche Käufe von Produkten mit geringem Volumen und hoher Nachfrage

Wenn Sie feststellen, dass Sie einen verdächtig hohen Prozentsatz Ihres Produktbestands an eine überraschend kleine Kundengruppe verkaufen, stecken womöglich Inventory-Hoarding-Bots dahinter. Einige dieser Bots beschränken sich darauf, Warenkörbe zu füllen und damit legitime Kunden zu blockieren. Andere kaufen Ihren Warenbestand auf, um ihn zu einem höheren Preis auf anderen Websites weiterzuverkaufen.

Zunahme von Kundenbeschwerden

Ein Anstieg der Support-Tickets im Zusammenhang mit Kontosperrungen und betrügerischen Transaktionen könnte ein Anzeichen für Credential-Stuffing-Bots sein. Diese Bots übernehmen legitime Benutzerkonten mit Informationen, die sie aus früheren Datenlecks gewonnen haben. Solche Betrugsgeschäfte beeinträchtigen nicht nur das Kundenerlebnis, sondern überlasten auch Ihre Server, was eine höhere Seitenladedauer zur Folge hat. Sie können sogar dazu führen, dass Ihre Website nicht mehr erreichbar ist.

Zunahme der fehlgeschlagenen Anmeldeversuche

Jeder Kunde gibt hin und wieder sein Passwort falsch ein. Wenn Sie aber plötzlich eine starke Zunahme von fehlgeschlagenen Anmeldeversuchen registrieren, haben Sie sehr wahrscheinlich ein Bot-Problem. Einige Credential-Stuffing-Bots versuchen, mit gestohlenen Anmeldeinformationen auf legitime Kundenkonten zuzugreifen. Einfacher und beliebter sind aber Brute-Force-Angriffe. Dabei unternehmen Bots in kürzester Zeit unzählige Anmeldeversuche mit Tausenden von beliebten Benutzernamen und Passwörtern aus ihren Verzeichnissen. Wenn ein Bot die zulässige Anzahl von fehlgeschlagenen Anmeldeversuchen für ein bestimmtes Konto überschreitet, wird der echte menschliche Besitzer dieses Kontos ausgesperrt, bis das Problem behoben ist – ein erhebliches Benutzererlebnisproblem.

Geringer Ertrag für Werbeausgaben

Digitale Werbung kann ein wirksames Instrument sein, um Besucher auf Ihre Website zu lenken, aber sie ist auch eine lukrative Waffe für schädliche Bots. Viele Traffic-Bots ahmen das Verhalten menschlicher Benutzer nach: Sie klicken wiederholt auf Ihre Anzeigen, um Ihre Pay-per-Click-Ausgaben (PPC) in die Höhe zu treiben, und springen dann ab, ohne etwas zu kaufen. Obwohl einige Werbeplattformen Machine Learning-Algorithmen zur Eindämmung von Klickbetrug einsetzen, bleibt ein Großteil unentdeckt. Aus diesem Grund ist es wichtig, vorausschauend jeden Klick zu überwachen, der über Ihre Anzeigen erfolgt.

Verzerrte Seitenaufrufe

Wenn Ihre Seitenaufrufe ohne erkennbaren Grund plötzlich in die Höhe schnellen, könnten schädliche Bots die Ursache sein. Traffic-Spitzen können von menschlichen Benutzern verursacht werden, wenn Sie gerade ein neues Produkt eingeführt oder eine Werbung für ein Event gestartet haben. Aber die Betreiber bösartiger Bots werden immer geschickter darin, Content-Scraping-Bots genau dann einzusetzen, um Ihre Inhalte zu stehlen und Ihre aggregierten Analysedaten negativ zu beeinflussen.

Plötzlicher Anstieg der Neukontenzahl

Wenn aus heiterem Himmel Hunderte oder sogar Tausende neuer Benutzerkonten auftauchen, stecken womöglich Bots hinter dem Zustrom. Mit diesen gefälschten Profilen können Bots Ihre öffentlichen Bewertungen spammen und zahlreiche andere Formen von Betrug begehen. Dies gefährdet nicht nur Ihren Umsatz und Ihre Nutzerbindung, sondern auch die Glaubwürdigkeit Ihrer Marke.

Nicht genehmigter Duplicate Content auf fremden Websites

Wenn fremde Websites Ihre Inhalte zur Verfügung stellen, kann das durchaus positiv sein. Doch eine plötzliche Zunahme an echtem Duplicate Content ist ein Anzeichen für Content-Scraping-Bots. Diese Bots stehlen Daten, die Sie aufwendig zusammengestellt und kuratiert haben. Sie ermöglichen betrügerischen Website-Betreibern, diese Daten auf ihren eigenen Domains zu hosten und so ihren Traffic zu steigern, während Ihr eigener leidet.

Zugriffe aus ungewöhnlichen Regionen

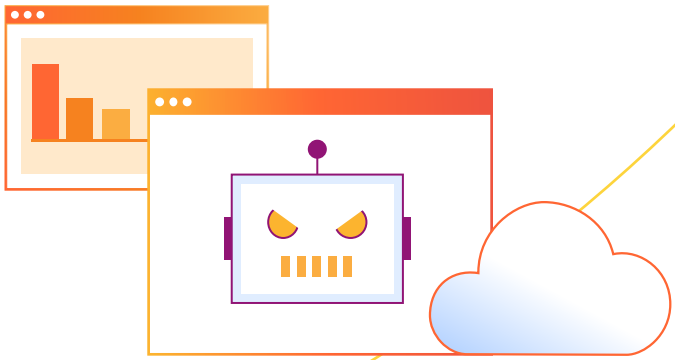
Plötzliche, von unerwarteten Regionen ausgehende Zugriffsspitzen können auf schädliche Bots hinweisen. Das gilt vor allem, wenn sich die Aktivität verstärkt auf Regionen konzentriert, in denen Ihre Kunden nicht wohnen oder Ihre Dienste nicht verfügbar sind. Achten Sie auf alle verdächtigen Aktivitäten, bei denen kein augenscheinlicher Zusammenhang mit Ihrer üblichen Nutzerbasis besteht.

Zugriff aus gewohnten Regionen zu ungewöhnlichen Zeiten

So wie Zugriffsspitzen aus unerwarteten Regionen auf bösartige Bots hindeuten können, sind Zugriffsspitzen aus unverdächtigen Regionen zu ungewöhnlichen Zeiten möglicherweise ein Anzeichen für Bots, die sich als regelmäßige Benutzer ausgeben. Wenn Sie beispielsweise mitten in der Nacht einen Anstieg der Aktivitäten in einer Ihrer gewohnten Regionen feststellen, sollten Sie sich diesen Traffic genauer ansehen.

Ein Anstieg in der Anzahl fehlerhafter Kartenprüfungen

Ein besonders bedrohliches Anzeichen für bösartige Bots ist ein Anstieg bei Kreditkartentransaktionen, die nicht validiert werden können. Credit-Card-Stuffing-Bots testen Tausende von gestohlenen Kreditkartennummern, um eine zu finden, die funktioniert. Dafür tätigen sie Einkäufe mit geringem Wert auf weniger sicheren Websites, bevor sie größere Transaktionen auf größeren Websites durchführen oder die validierten Kartennummern im Dark Web verkaufen. Ihre Website kann an jedem Punkt dieses Plans betroffen sein – und wenn die fehlgeschlagenen Transaktionen ein exorbitantes Ausmaß erreichen, nimmt Ihr Zahlungsanbieter Sie möglicherweise in Regress.



2. https://www.entrepreneur.com/article/313943

Taktiken für die Bekämpfung von Bots

Da kein Bot-Angriff dem anderen gleicht, müssen in der Regel mehrere Taktiken kombiniert werden, um sie alle zu stoppen. Dabei sollten Sie die folgenden Strategien in Betracht ziehen:

Blockieren Sie schädliche Bots, sobald Sie sie bemerken

Die naheliegendste Maßnahme gegen einen Bot zählt auch zu den effektivsten: Blockieren Sie einfach den gesamten Traffic, den Sie auf böswillige Bot-Aktivitäten zurückführen können. Schon diese Taktik für sich genommen ermöglicht erhebliche Kosteneinsparungen bei Bandbreite und Speicher – ganz abgesehen davon, dass Sie sich das Verbrauchervertrauen bewahren und den Ruf Ihrer Marke schützen. Denken Sie aber auch daran, dass ein hochmotivierter Bot-Betreiber seine Taktik ändern und es später mit einer anderen Angriffsstrategie erneut versuchen könnte.

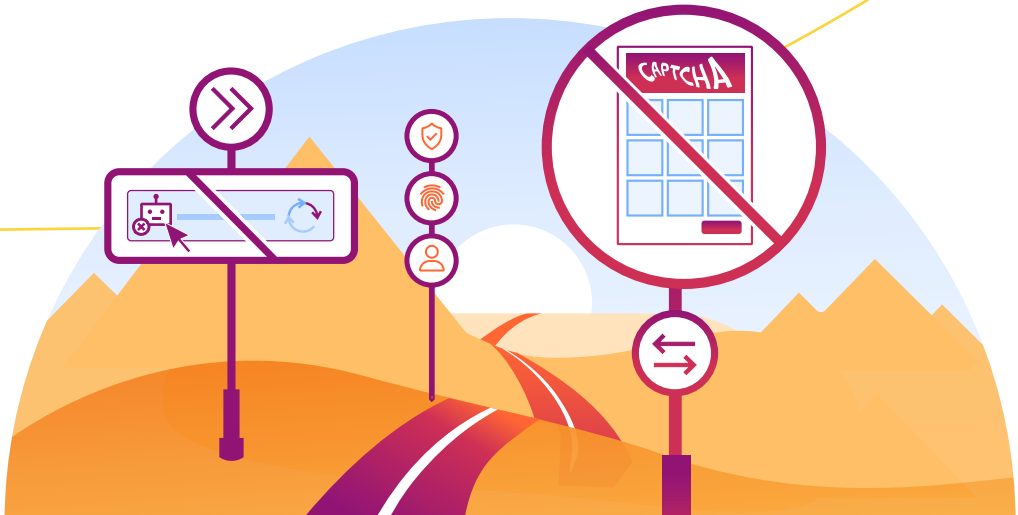
Setzen Sie alle Ihnen bekannten vertrauenswürdigen Bots auf eine Positivliste

Während Sie schädliche Bots erkennen und blockieren, müssen Sie gleichzeitig unbedingt dafür sorgen, dass vertrauenswürdige Bots von Suchmaschinen und Partnern Ihre Website weiterhin auslesen können. Dadurch bewahren Sie Ihr gutes SEO-Ranking. Außerdem wird damit gewährleistet, dass der legitime Kunden-Traffic von Drittanbietern, die Traffic an Sie weiterleiten, reibungslos fließt. Eine Positivliste erleichtert auch das Festlegen von Bot-Blockierregeln, die den Zugriff echter Besucher nicht beeinträchtigen.

Stellen Sie verdächtige Bots auf die Probe

Sobald Sie ein Muster verdächtiger Anmeldungen, geringer Seitentiefe oder Verweilzeiten, fehlgeschlagener Kreditkartenprüfungen oder eines anderen typischen Bot-Verhaltens bemerken, sollten Sie unbedingt einen Sicherheitstest einsetzen. In der Vergangenheit wurde das Senden von CAPTCHA-Abfragen als Best Practice angesehen. Viele hochentwickelte Bots können diese Aufgaben jedoch inzwischen sogar schneller und genauer lösen als menschliche Benutzer.

Heutzutage ist der beste Ansatz die Verwendung von CAPTCHA-freien Challenges, bei denen die „Challenge“-Software eine Vielzahl von Faktoren berücksichtigt, um festzustellen, ob der Benutzer wirklich ein Bot ist (z. B. Netzwerk-, Geräte- und JavaScript-Fingerprints). „No CAPTCHA“-Prüfungen wie diese sind idealerweise in eine vollständige Bot-Management-Lösung integriert, um maximale Genauigkeit zu erzielen (weitere Informationen dazu im Abschnitt „Fazit“)



Begrenzen Sie die Zahl der Benutzeranfragen

Rate Limiting kann eine wirksame Technik sein, um weniger komplexe Bots in Schach zu halten. Legen Sie Obergrenzen für die Anzahl der Anfragen fest, die eine IP-Adresse an Ihre Website senden kann. Damit verhindern Sie viele einfache Brute-Force-Angriffe durch Bots, die versuchen, sich mit Tausenden von Wörterbuchbegriffen und gängigen Passwörtern anzumelden. Allerdings können moderne, weiter entwickelte Bots die Anzahl ihrer Anfragen knapp unter der von Ihnen festgelegten Obergrenze halten. Dadurch bleiben sie unentdeckt und können weiterhin Schaden anrichten.

Führen Sie detaillierte Protokolle über den gesamten Website-Traffic

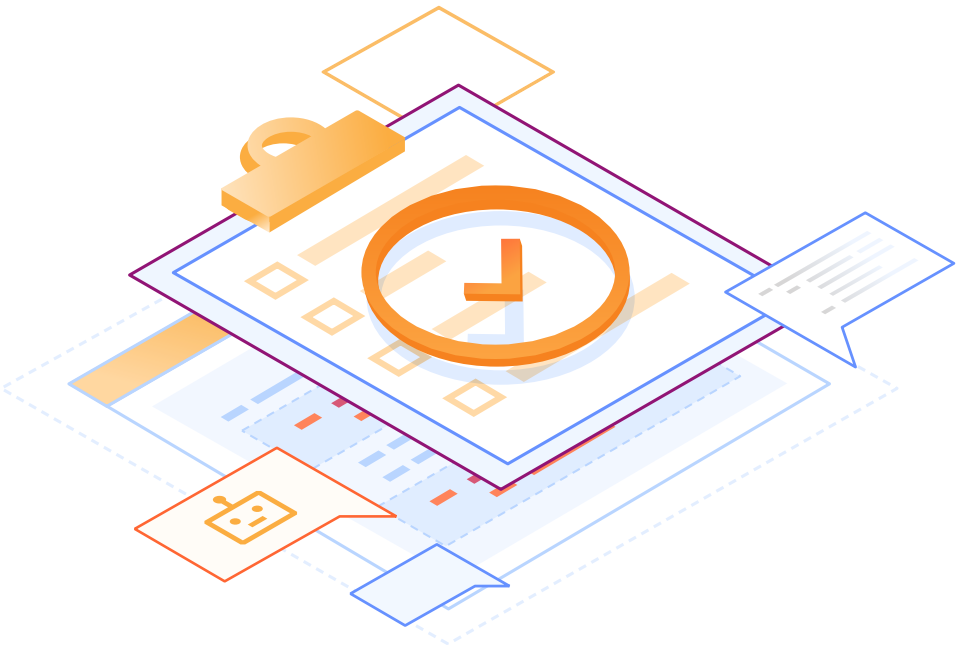
Wahrscheinlich führen Sie bereits tägliche Protokolle über Seitenaufrufe und Kontoanmeldungen. Doch um unauffälligere Aktivitätsmuster zu erkennen, können detailliertere Protokolle mit Benutzerinformationen (wie IP-Adressen, Browser, Geräte, Betriebssysteme, Standortdaten, Referrer, Netzwerke und Seitenaufrufe) von unschätzbarem Wert sein. Protokolle können Ihnen ein klares Bild des Verhaltens von Bots auf Ihrer Website vermitteln. Das gibt Ihnen die Möglichkeit, wirksamere Sicherheitsrichtlinien festzulegen. Darüber hinaus sind Protokolle oft unerlässlich für Reporting und Compliance, falls bei Ihnen tatsächlich ein Datenleck vorliegt.

Leiten Sie Bots zu alternativen Inhalten um

Wenn Sie relativ sicher sind, dass es sich bei einer bestimmten Traffic-Quelle um einen Bot handelt, präsentieren Sie ihm alternative Inhalte, die seine Rechenressourcen beanspruchen. Sie können sogar Content-Scraping-Bots mit falschen Daten – z. B. fehlerhaften Preisinformationen – füttern, wodurch diese für ihre Betreiber nutzlos werden. Mit solchen Methoden verschaffen Sie sich Zeit, um das Verhalten des Bots zu beobachten, sein Aktivitätsmuster zu verstehen und eine Strategie vorzubereiten, um ihn endgültig unschädlich zu machen.

Verlangen Sie von allen Benutzern zusätzliche Authentifizierung

Mit zunehmender Häufigkeit von Bot-Angriffen ergreifen immer mehr Websites erhöhte Sicherheitsmaßnahmen – selbst bei zulässigen Anmeldungen menschlicher Benutzer. Bei der Zwei-Faktor-Authentifizierung (2FA) beispielsweise müssen Benutzer ihre Identität auf mehreren Geräten oder Konten bestätigen. Einmal-Passwörter (One-time Passwords, OTPs) hingegen können Credential-Stuffing-Bots entmutigen, weil sie das Knacken von Konten erschweren. Denken Sie jedoch daran, dass diese Verfahren die Nutzererfahrung beeinträchtigen können, weil sie den Aufwand bei der Anmeldung erhöhen.

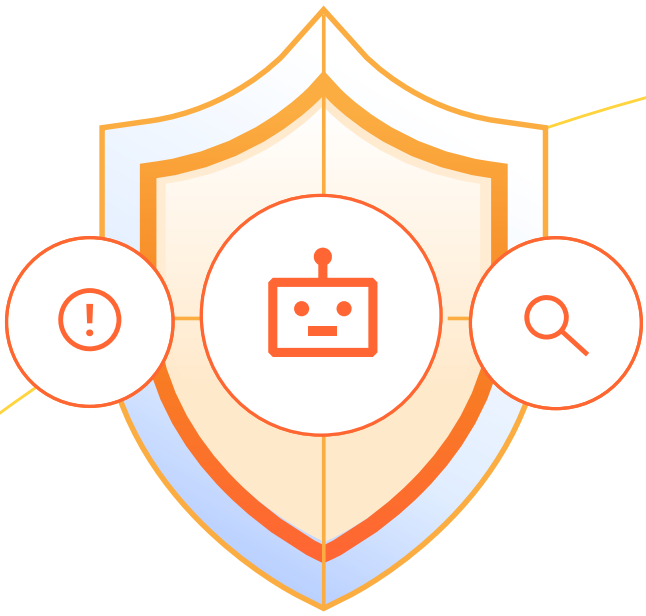


Fazit

Während Sie diese Methoden ausloten, sollten Sie eines nicht vergessen: Für sich genommen wird keine von ihnen in der Lage sein, alle Bots aufzuhalten. Um Ihr Unternehmen zu schützen, müssen Sie wahrscheinlich mehrere Taktiken gleichzeitig anwenden – und zusätzlich auf erweiterte multivariable Musteranalysen zurückgreifen. Cloudflare Bot-Management hilft Unternehmen in einer Vielzahl von Branchen dabei, diesen mehrgleisigen Ansatz zu verfolgen. Dieser Dienst ist in das umfassendere Cloudflare-Netzwerk integriert, das über 25 Millionen Websites und Webanwendungen unterstützt und mehr als 200 Städte weltweit umfasst.

Dank der Nutzung kontinuierlicher Bedrohungsdaten aus diesem Netzwerk kann Cloudflare Bot-Management Verhaltensanalysen, Machine Learning und Fingerprinting bieten und dadurch die Bekämpfung schädlicher Bots erheblich erleichtern. Darüber hinaus bietet Cloudflare Turnstile an, eine nahezu reibungslose, CAPTCHA-freie Bot-Challenge, die mit nur wenigen Zeilen Code in jede Webanwendung integriert werden kann.

Erfahren Sie mehr über das Cloudflare Bot-Management.



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-6333.2024SEPT03