AKAMAI-PRODUKTBESCHREIBUNG

Bot Manager

Wem vertrauen Sie? Und ebenso wichtig: Wer vertraut Ihnen? Sie müssen darauf vertrauen, dass Verbraucher, Partner und Bots bei Onlinetransaktionen auch wirklich die sind, für die sich ausgeben. Leider versuchen viele Bots – die bis zu 70 % des Traffics einer Website ausmachen können – sich als legitime Nutzer auszugeben, Ihr geistiges Eigentum zu stehlen und Ihren Prozessen zu schaden. Akamai Bot Manager bietet ihnen Transparenz und Kontrolle über Bots, damit Sie Ihr Unternehmen schützen können und somit das Vertrauen in Ihre Onlinebeziehungen wahren.

Unternehmen setzen für Onlineeffizienz zunehmend auf gute Bots, mit denen sie Interaktionen mit Verbrauchern, Partnern, Lieferanten und Dritten automatisieren. Im Gegenzug müssen Sie den Einfluss dieser Bots auf die Website-Performance und das Kundenerlebnis managen.

Denn auch Betrüger und Kriminelle setzen vermehrt auf Automatisierung. Sie skalieren Botnets für folgende Operationen:

- Abgreifen von Inventar vor dem Verkauf an Kunden
- Starten von Credential-Stuffing-Angriffen
- Diebstahl von Treuepunkten und Geschenkkarten
- Ausnutzen von Schwachstellen in der Geschäftslogik
- Angriffe auf Unternehmen, um Websites zu verlangsamen und die Kosten zu erhöhen

Wie können Sie genau wissen, dass Sie Ihren Onlineinteraktionen vertrauen können, wenn Bot-Betreiber derartige Anstrengungen unternehmen, um Ihnen und Ihren Kunden zu schaden? Und wie können Sie anderen zeigen, dass sie Ihnen vertrauen können?

Dank der herausragenden Funktionen von Bot Manager für die Bot-Erkennung und -Abwehr können Sie automatisierte Prozesse effizienter und sicherer ausführen. Damit wächst das Vertrauen in Sie und Ihr gesamtes Ökosystem.

Vertrauen beginnt mit Akamai für Ihr Bot-Management

Aufgrund unserer globalen Stärke können Sie Akamai sowohl in technologischer als auch in unternehmerischer Hinsicht vertrauen. Zu unseren Kunden zählen mehr als die Hälfte der Global 500, wir verfügen über mehr als 4.167 Points of Presence in über 131 Ländern und verzeichnen einen jährlichen Umsatz von mehr als 3,6 Milliarden US-Dollar. All diese Stärken fließen in den Bot Manager ein, den wir kontinuierlich weiterentwickeln. So stellen wir sicher, dass seine Leistung nicht nachlässt und er Bots und Verschleierungstechniken stets einen Schritt voraus ist.

VORTEILE FÜR IHR UNTERNEHMEN

Vertrauen stärken: und das gegenseitig
Erkennen Sie legitime Interaktionen, reduzieren Sie Reibungspunkte für Nutzer und schützen Sie sie vor Betrug – für mehr Vertrauen zwischen Verbrauchern, Partnern und Ihrem Unternehmen.

Kosten durch Wiederherstellungsmaßnahmen verringern
Reduzieren Sie Kosten und die Beanspruchung von Ressourcen für das Überprüfen kompromittierter Konten, das Ersetzen gestohlener Accounts, das Bearbeiten von Nutzerbeschwerden und anderer Nachwirkungen von Bot-Angriffen.

Operative Kontrolle verbessern
Verbessern Sie Ihre Effizienz, verringern Sie geschäftliche und finanzielle Risiken, kontrollieren Sie IT-Ausgaben und managen Sie Partner-Bots strategisch.

Bessere, datengesteuerte Entscheidungen treffen
Dank detaillierter Analysen und detailliertem Reporting können Sie kreative und effektive Entscheidungen hinsichtlich Customer Journeys, Sicherheitsstruktur, Risikotoleranz und IT-Prozessen treffen.

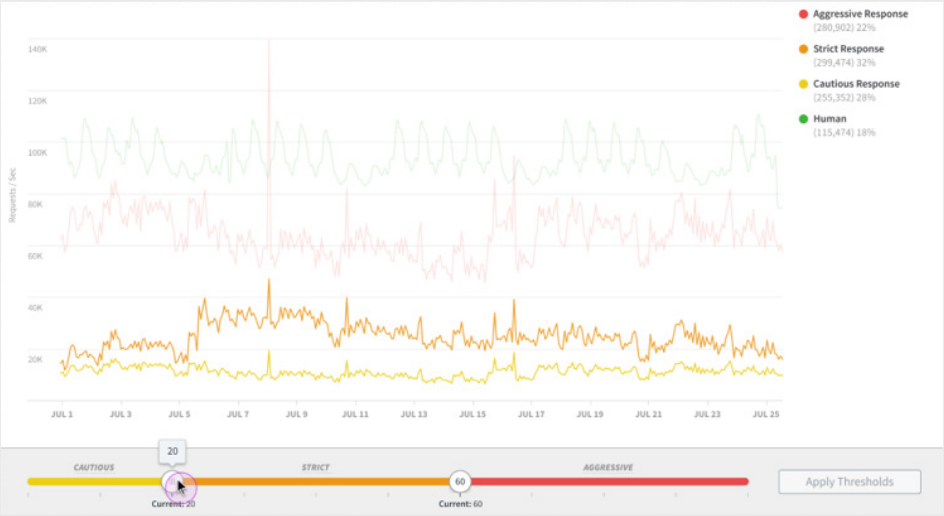
©2023 Akamai Technologies | Support-Website | Veröffentlicht: 10/23

Bot Manager verwendet für die Bot-Erkennung und -Abwehr patentierte Technologien, mit deren Hilfe der Bot direkt gestoppt wird und gar nicht erst auf Ihre Website gelangt. Und wir arbeiten unermüdlich daran, dass Sie auch dann geschützt bleiben, wenn sich Bedrohungen stetig weiterentwickeln. Erkenntnisse unserer Experten für Bedrohungsinformationen werden automatisch in die Erkennungs- und Analysealgorithmen des Bot Manager integriert – Sie müssen sich also nicht um zusätzliche Upgrades oder Erweiterungen kümmern.

Bot Manager schützt Ihr Unternehmen an Interaktionspunkten mit Dritten, einschließlich Web-Endpunkten sowie den Endpunkten nativer Apps und APIs. Es besteht selbst dann ein Schutz durch Bot Manager, wenn eine Anfrage die Domain wechselt. Wenn Sie über mehrere Marken oder Unternehmen verfügen, folgt Bot Manager der Erstanfrage über die gesamte Interaktion hinweg und sorgt damit für fortlaufenden Schutz.

Bot Manager KI-Framework

Bot Manager basiert auf einem KI-Framework (künstliche Intelligenz), das inline auf der Akamai Connected Cloud läuft. Dadurch erkennt Bot Manager den Traffic direkt an der Edge, wo sich Nutzer erstmals mit einer Anwendung verbinden. Damit erhalten Sie hinsichtlich Trafficmuster, -typen und -volumen „saubere“ Daten. Über das gesamte Netzwerk hinweg verzeichnet Akamai durchschnittlich 37 Milliarden Bot-Anfragen pro Tag.



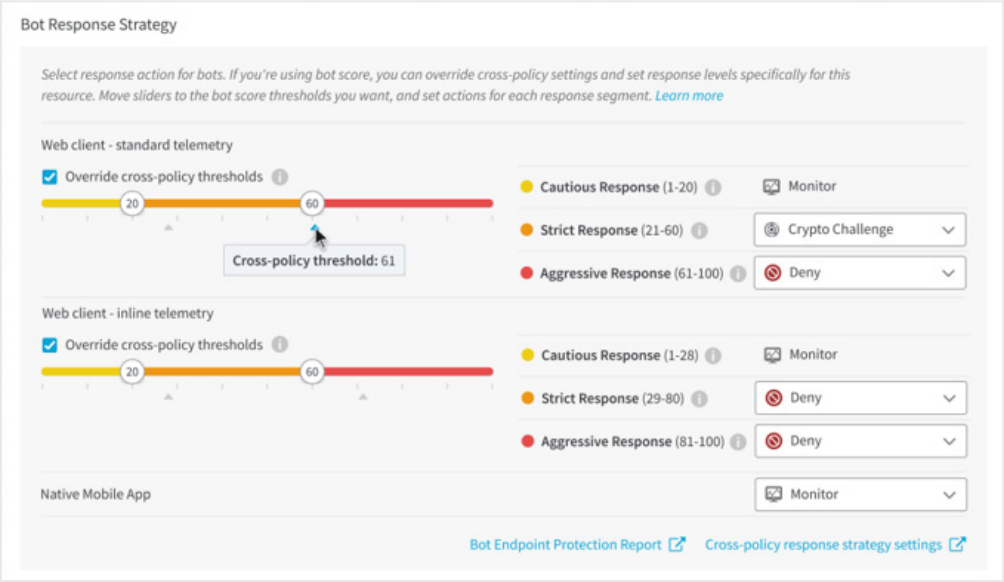
KI, maschinelles Lernen und Threat Intelligence

Durch das Sammeln „sauberer Trafficdaten“ über eine Vielzahl von Datentypen hinweg und in großen Volumina werden unsere Algorithmen für maschinelles Lernen (ML) trainiert, damit sie noch genauer werden. Im gesamten Akamai-Netzwerk beobachten wir täglich Traffic von 1,3 Milliarden unterschiedlichen Geräten mit einem Spitzentraffic von 164 Tbit/s. Durch die Erkenntnisse aus diesen Daten können unsere Algorithmen mehr und schneller lernen. Außerdem verfolgt unser Bedrohungsforschungsteam aus mehr als 400 Experten kontinuierlich die neusten Angriffsmuster- und Technologietrends sowie Innovationen und Umgehungsmaßnahmen, um die Erkennung zu verbessern. Die Bedrohungsforschung bei Akamai analysiert Tag für Tag 662 TB neuer Angriffsdaten – gegenüber 290 TB im Jahr 2021.

Zusätzlich zu den leistungsstarken KI- und ML-Techniken von Akamai bieten wir nun die Möglichkeit, kundenspezifische Modelle zu entwickeln. Diese Deep-Learning-Modelle untersuchen die komplexesten Angriffe, die wir auf großen Markenwebsites beobachten, welche beliebte Angriffsziele darstellen. Das Modell wandelt dann das Gelernte in fortschrittliche Algorithmen um und kann so Abwehrmaßnahmen gegen neuartige Angriffe innerhalb von Minuten statt Tagen oder Wochen implementieren.

Bot Score: Bewerten Sie jeden Bot bei jeder Erkennung

Bot Score kombiniert ganzheitlich alle Erkennungsauslöser, um komplexe Bots zu identifizieren und Ihnen eine genauere Bewertung jeder einzelnen Anfrage zu ermöglichen. Dadurch wird die Gesamteffizienz des Systems optimiert – und das ohne zusätzliche Latenz. Darüber hinaus können Sie eine Reaktionsstrategie auf der Grundlage von Bewertungsstufen definieren.



Innovative Challenges

Die Kombination der Bot-Score-Funktion von Bot Manager mit hochmodernen Challenges ermöglicht ein automatisches Handeln dank vordefinierter Schwellenwerte und Reaktionsmaßnahmen. Mit unseren für Menschen unsichtbaren Challenges verschiebt sich die Beweislast von legitimen menschlichen Nutzern hin zu Bots. Die Crypto Challenge zwingt Bots dazu, CPU-Zyklen für kryptografische Puzzles aufzuwenden, die in kürzester Zeit gelöst werden müssen. Dadurch werden raffinierte Bot-Angriffe extrem verlangsamt und die Kosten für die Angreifer schnellen in die Höhe. Die Interstitial Challenge erfordert von den Clients einen Nachweis darüber, dass sie das Speichern von Cookies und JavaScript unterstützen. Wenn sie dies nicht können, zwingt Bot Manager ihnen eine Zeitstrafe sowie eine von Ihnen zur Abwehr ausgewählte Maßnahme auf.

Angriffsschutz mit Netzwerkeffekt

Wir schützen einige der größten und angesehensten Unternehmen weltweit, die oftmals Ziel der fortschrittlichsten Bot-Betreiber sind. Wenn bei einem Kunden ein neuer Bot entdeckt wird, werden die Daten zu diesem Bot innerhalb von Minuten sowohl der Bibliothek bekannter Bots als auch unserem einzigartigen „Katapultalgorithmus“ für alle Kunden hinzugefügt. Dieser Netzwerkeffekt ermöglicht Kunden nicht nur ein effektives Bot-Management, sondern hilft uns darüber hinaus, einige Bots präventiv an Angriffen gegen andere Kunden zu hindern.

Schnelle, unkomplizierte Bereitstellung

Die Inline-Architektur des Bot Manager sorgt für eine schnelle und nahtlose Bereitstellung. Zudem arbeitet Bot Manager von Beginn an akkurat und entdeckt Bots in Echtzeit ohne Latenz oder Auswirkungen auf die Website- oder Netzwerkperformance. Dank der herausragenden Kapazitäten des Akamai-Netzwerks wächst der Bot Manager mit Ihnen. Über welche Kapazitäten verfügt das Akamai-Netzwerk? Der Traffic in unserem Netzwerk übersteigt jeden Tag einen Spitzenwert von 100 Tbit/s. Am 14. Dezember 2022 wurde ein bisheriger Höchstwert von 261,21 Tbit/s erreicht.

©2023 Akamai Technologies | Support-Website | Veröffentlicht: 10/23

Wichtige Funktionen

Verzeichnisse bekannter Bots: Bot Manager antwortet automatisch angemessen auf bekannte Bots, und wir arbeiten kontinuierlich daran, unser Verzeichnis mit derzeit 1.750 bekannten Bots zu aktualisieren.

Hochentwickelte, dynamische Bot-Erkennung: Bot Manager erkennt unbekannte Bots dank einer Vielzahl an KI-Modellen und -Techniken sowie Modellen und Methoden für ML von ihrer ersten Interaktion an. Dazu zählen Analysen des Nutzerverhaltens, Browser-Fingerprinting, automatisierte Browser-Erkennung, HTTP-Anomalie-Erkennung, hohe Anfrageraten und vieles mehr. Die dynamische Verschleierung von Code und Telemetrie durch Bot Manager schützt vor Rekonstruktion und sorgt dafür, dass Bot Manager auch langfristig effektiv ist.

Modell zur Bewertung: Das Modell von Bot Score wertet jede Anfrage mit jeder Bot Manager Premier-Erkennung aus. Anschließend wird berechnet, mit welcher Wahrscheinlichkeit die Anfrage von einem Bot stammt, woraufhin eine Bewertung von 0 (definitiv ein Mensch) bis 100 (definitiv ein Bot) vergeben wird.

Erkennung von Browser-Imitation: Bot-Betreiber versuchen häufig, bestimmte Browser zu imitieren, um sich der Erkennung zu entziehen. Wir haben unsere Erkennung von Browser-Imitation weiterentwickelt. Sie ist nun äußerst genau und bedarf keiner regelmäßigen Abstimmung, sodass Kunden weniger False Negatives erhalten als mit anderen Erkennungsmethoden.

Nutzerdefinierte Einstellung pro Endpunkt: Mit der Bot-Score-Funktion lassen sich für jeden Endpunkt unterschiedliche Antworten festlegen. Sie können beispielsweise die Antwort „Vorsichtig“ (beobachten/überwachen) auf Bots anwenden, deren Ergebnisse auf Ihrer Suchseite 35 oder weniger betragen. Gleichzeitig können Sie den Schwellenwert für Anfragen auf Ihrer Anmeldeseite auf 20 herabsetzen.

Simulator für die Antwortoptimierung: Ihre strategischen Antworten können je nach Endpunkt und Risikotoleranz Ihres Unternehmens angepasst werden. Dank Bot Score können Sie Ihre Optimierung simulieren, bevor Sie sie in die Praxis umsetzen. Auf diese Weise lassen sich die Auswirkungen der veränderten Schwellenwerte basierend auf Ihrem vergangenen Traffic visualisieren.

Automatische Feineinstellung: Verringern Sie die Notwendigkeit menschlicher Eingriffe bei der Optimierung, selbst wenn sich Bots weiterentwickeln. Bot Manager lernt die normalen Trafficmuster Ihrer Website(s) und passt die Erkennung automatisch an, um potenziell falsch klassifizierte Anfragen zu vermeiden.

Nuancierte Maßnahmen: Verbessern Sie Ihre Bot-Abwehr mit Maßnahmen, die über bloßes Blockieren/Zulassen hinausgehen, wie beispielsweise Bereitstellen alternativer Inhalte, Lösen von „Challenges“, Verlangsamen und vieles mehr.

Detailliertes Reporting und detaillierte Analysen: Treffen Sie Entscheidungen basierend auf Daten aus dem Echtzeit- bzw. Verlaufs-Reporting des Bot Manager. Sie erhalten Erkenntnisse zu Trends und detaillierte Analysen einzelner Bots oder anderer Segmente Ihres Bots-Traffics. Darüber hinaus können Sie Ihren Bot-Traffic mit dem Ihrer Wettbewerber und aller anderen Akamai-Kunden vergleichen.

Managed Security Service (optional): Optimieren Sie Bot Manager, ohne dafür Ihr eigenes Team beanspruchen zu müssen. Ihre persönlichen Experten von Akamai überwachen Empfehlungen für Maßnahmen und stellen diese proaktiv zur Verfügung. Außerdem leisten sie Ihnen bei Sicherheitsvorfällen Notsupport.

Risikobewusstes Bot-Management

- Unterstützen Sie die Ziele Ihres Unternehmens, indem Sie Ihre Bot-Reaktionen an die Risikotoleranz Ihres Unternehmens anpassen.
- Ändern Sie Schwellenwerte, um langfristige Ziele zu erfüllen und auf einzelne Ereignisse wie Flash-Sales reagieren zu können.
- Legen Sie strategische Antworten je nach Endpunkt fest, zum Beispiel aggressive Maßnahmen auch bei niedrigerer Risikobewertung für hochwertige Endpunkte.

Weitere Informationen erhalten Sie von Ihrem Akamai-Vertriebsmitarbeiter oder unter Akamai.com.

©2023 Akamai Technologies | Support-Website | Veröffentlicht: 10/23