CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

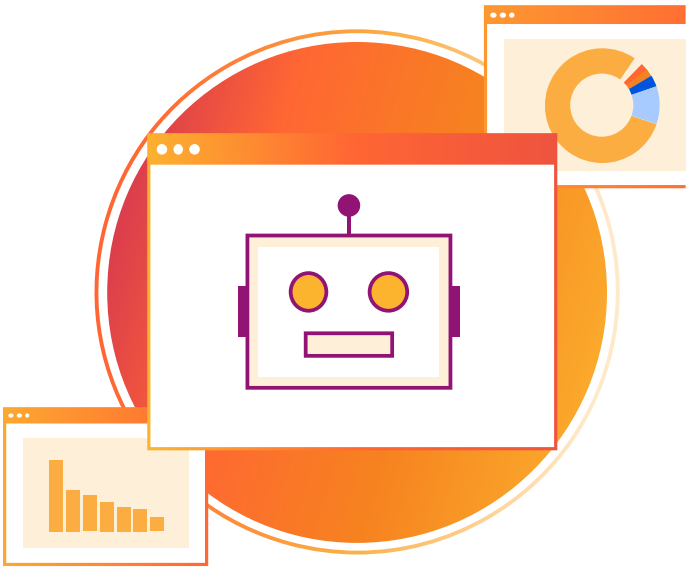
4 estrategias para gestionar bots maliciosos

Evita daños costosos y la pérdida de ingresos debidos a los bots no deseados

Los bots son omnipresentes en Internet

Hoy día, los bots son habituales en Internet porque ayudan a automatizar tareas importantes. Se estima que entre el 40 % y el 50 % del tráfico total de Internet está basado en bots, y muchos de ellos realizan funciones empresariales legítimas.

Sin embargo, también los delincuentes a menudo los utilizan para atacar propiedades web y causar graves daños. Los bots maliciosos pueden robar datos, acceder de forma ilegítima a cuentas, enviar datos basura en formularios en línea y realizar otras actividades maliciosas. Estos bots maliciosos malgastan valiosos recursos de proceso y de los sitios, roban datos y causan sesgos en los análisis del tráfico.



¿Qué es la gestión de bots?

La gestión de bots consiste en bloquear el tráfico de bots no deseados o malintencionados y, al mismo tiempo, permitir el acceso de los bots útiles a las propiedades web. Para ello, la gestión de bots detecta la actividad de bots, distingue entre los comportamientos legítimos y los no deseables e identifica los orígenes de las actividades malintencionadas.

¿Por qué es importante?

La gestión de bots es necesaria, porque, si no se controlan, pueden causar importantes y costosos problemas. Al intentar filtrar el tráfico de bots maliciosos que se dirige a sus propiedades web, las organizaciones deben asegurarse de que no bloquean los bots necesarios, como los bots de rastreo de los motores de búsqueda.

¿Qué podemos hacer?

Identificar y bloquear los bots maliciosos antes de que se inicie cualquier ataque es un elemento esencial de cualquier buena estrategia de seguridad. Hemos compartido cuatro historias de clientes reales de Cloudflare que han abordado sus desafíos de gestión de bots con cuatro estrategias distintas utilizando productos de Cloudflare.

Bloquear los bots

Este enfoque exige atención, ya que muchos procesos empresariales legítimos, como la indexación de los motores de búsqueda, requieren bots para poder acceder a los recursos de las empresas.

Bloquear los bots		
Desafíos	**Solución**	**Resultados**
Una empresa de iGaming observó un aumento considerable de las quejas de los usuarios. Los hackers habían entrado en sus cuentas y les habían robado la información de sus tarjetas de crédito. Los delincuentes utilizaban bots automatizados para obtener a la fuerza bruta las credenciales de inicio de sesión, acceder a las cuentas de los usuarios y, finalmente, tomar su control.	El equipo de seguridad aplicó el servicio de **limitación de velocidad** junto con el de **gestión de bots avanzada** para detectar si se producían varios intentos de inicio de sesión en un breve intervalo de tiempo. Cuando detectaba un comportamiento inusual, la limitación de velocidad empezaba a bloquear automáticamente las solicitudes maliciosas. Desde la implementación de la función de limitación de velocidad, la empresa de iGaming no ha sufrido ningún ataque de relleno de credenciales.	Todas las empresas deben encontrar el equilibrio entre una seguridad estricta y una experiencia de usuario óptima. Las herramientas adecuadas pueden contribuir a detectar y evitar el tráfico de bots maliciosos y, al mismo tiempo, minimizar los falsos positivos y los obstáculos para los usuarios reales.

Ralentizar al enemigo

Esta técnica maximiza el tiempo de respuesta para todas las solicitudes sospechosas enviadas en la red.

Ralentizar al enemigo		
Desafíos	**Solución**	**Resultados**
Una empresa de apuestas deportivas observó una reducción considerable de las transacciones. Al analizar el problema, identificaron la actividad de bots maliciosos, que se estaban apropiando de las apuestas en su sitio web y utilizando esa información para obtener una ventaja competitiva.	La empresa no bloqueó los bots porque los delincuentes encontrarían una forma de saltarse el bloqueo. Como alternativa, ralentizaron la obtención de datos sobre las apuestas. Utilizaron la **anulación del encabezado** para marcar las solicitudes sospechosas según el análisis de la **gestión de bots**, y a continuación scripts de **Workers** para reaccionar a estos encabezados y ralentizar las solicitudes.	Este método permitió a la empresa restaurar la actividad normal de los usuarios. Otros métodos son la utilización de los desafíos CAPTCHA para los volúmenes grandes de solicitudes o modificar periódicamente el código HTML. Estas acciones interrumpen el flujo de trabajo de los bots, por lo que la apropiación de contenido coherente resulta más complicada.

Engañar a los bots

Aunque muchas empresas implementan medidas defensivas contra los bots, un atacante con la determinación suficiente puede evadirlas. Como alternativa, algunas empresas deciden contraatacar.

Engañar a los bots		
Desafíos	**Solución**	**Resultados**
Una empresa de apuestas deportivas intentaba encontrar una solución a los bots que se apropiaban de las apuestas en su sitio web. Tras considerar el problema, decidieron lanzar una solución con varios productos de Cloudflare que les permitiría proporcionar a los bots información aleatorizada.	Cuando el sistema veía que un bot malicioso había generado una solicitud, la aceptaba y generaba un nuevo flujo de trabajo: Solicitud → **WAF** (bot identificado) → **Gestión de bots** (clasificación de riesgo asignada) → **Workers** (generar datos aleatorizados) → **Workers** (envío de datos aleatorizados al bot)	El nuevo flujo de trabajo generaba nuevos datos aleatorizados que se devolvían a los bots maliciosos. Como resultado, los bots que venían a extraer apuestas e infringir daño obtenían datos inútiles, lo que les disuadía de intentar cualquier otro uso fraudulento.

Realizar análisis dinámicos

A medida que los bots son cada vez más sofisticados, es necesario que las empresas, antes de tomar medidas, recopilen datos sobre los bots y realicen análisis dinámicos. Estos objetivos pueden incluir la detección de registros incorrectos, apuestas, reclamaciones de bonificación, etc. Para garantizar un análisis exhaustivo, es posible que los equipos de seguridad deban combinar varias fuentes de datos, de herramientas tanto internas como externas, para analizar los parámetros del tráfico de bots.

Realizar análisis dinámicos		
Desafíos	**Solución**	**Resultados**
Una empresa de apuestas lanzó una campaña de marketing para atraer a nuevos usuarios ofreciendo recompensas si se registraban. Poco después del lanzamiento, observaron que bots estaban realizando registros falsos. La empresa ya contaba con algunas herramientas internas de análisis, pero no proporcionaban una visión global del comportamiento de los bots.	El equipo implementó la **gestión de bots avanzada** de Cloudflare con firmas JA3 para generar **registros sin procesar** de todo el tráfico de Internet que llegaba a la página de registro. Enriquecieron sus sistemas internos con puntuaciones de bots y firmas JA3, lo que les permitió una identificación más precisa de los bots.	Tras un análisis exhaustivo, la empresa pudo cancelar los registros falsos y evitar así que las estadísticas de los nuevos usuarios obtenidos estuvieran infladas. Añadieron análisis periódicos de bots, utilizando firmas JA3 en sus prácticas recomendadas.

Anticípate a los bots maliciosos

Gestión de bots de Cloudflare

Implementación sencilla
Sin configuración ni mantenimiento complejos

Baja latencia
Latencia media de <0,3 ms

Análisis enriquecidos
Correlaciona los registros de tráfico con otras fuentes de datos como SIEM o herramientas de inteligencia empresarial (BI)

Controles precisos
Ajusta las reglas, utiliza un generador visual de reglas o escribe tus propias reglas de comparación de patrones

Detén los bots maliciosos antes de que causen daños a tu negocio

Los bots son cada día más avanzados. A medida que las estrategias de los atacantes son cada vez más sofisticadas, la detección y el bloqueo de bots presentan limitaciones inherentes.
Hoy día, las empresas deben ajustar constantemente sus estrategias para hacer frente a las nuevas herramientas de los atacantes y, al mismo tiempo, encontrar el equilibrio adecuado entre una seguridad rigurosa y minimizar las molestias para los usuarios.

Sea cual sea la estrategia que decidas utilizar, asegúrate de que tu socio haya implementado un conjunto flexible de herramientas para gestionar los bots con eficacia. Para obtener más información sobre cómo Cloudflare puede ayudarte con los desafíos de los bots, ponte en contacto con nosotros para beneficiarte de una evaluación personalizada.

Información en la que puedes confiar

Cloudflare redirecciona mediante proxy aproximadamente el 20 % de todo el tráfico global de Internet, lo que proporciona mucha información en tiempo real sobre los comportamientos de los bots maliciosos en toda la red de Cloudflare.
Además, Cloudflare trabaja con distintos socios que comparten la información sobre credenciales de inicio de sesión robadas, lo que facilita la detección de los intentos de usurpación de cuentas antes de que causen una fuga de datos.

Empieza tu recorrido hacia una red más rápida, fiable y segura

Solicita una reunión

¿Aún tienes dudas?

Más información sobre Cloudflare