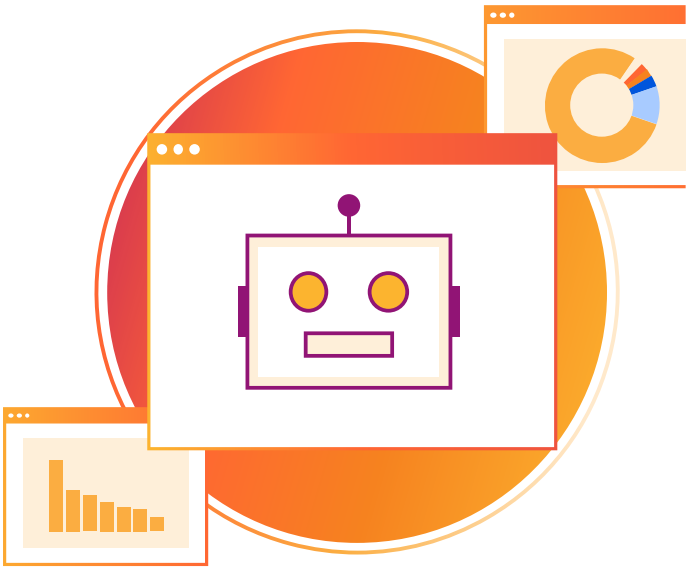
4 estrategias para gestionar los bots maliciosos

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

Los bots están en toda la Internet

Los bots son comunes en la Internet actual porque ayudan a automatizar tareas importantes. Se estima que entre el 40 % y el 50 % del tráfico total de Internet es generado por bots, y muchos de estos bots realizan funciones comerciales legítimas.

Sin embargo, los bots también son utilizados con frecuencia por delincuentes para atacar propiedades web y causar daños costosos. Los bots maliciosos pueden robar datos, acceder a las cuentas de los usuarios, enviar datos no deseados a través de formularios en línea y llevar a cabo otras actividades maliciosas. Estos bots maliciosos desperdician valiosos recursos informáticos y del sitio, roban datos y sesgan los análisis de tráfico.



¿Qué es la gestión de bots?

La gestión de bots consiste en bloquear el tráfico de bots no deseado o malintencionado de Internet, y permite al mismo tiempo el acceso de los bots buenos a las propiedades web. La gestión de bots consigue este objetivo al detectar la actividad de los bots, diferenciar entre el comportamiento deseado y no deseado de los mismos, e identificar las fuentes de la actividad no deseada.

¿Por qué es importante?

La gestión de bots es necesaria porque si no se controlan, estos pueden causar problemas masivos y costosos. Las organizaciones deben asegurarse de no bloquear bots necesarios, como los bots de rastreo de motores de búsqueda, al intentar filtrar el tráfico de bots maliciosos a sus propiedades web.

¿Qué se puede hacer?

Identificar y bloquear los bots maliciosos antes de que lancen ataques es un paso fundamental de cualquier buena estrategia de seguridad. Hemos compartido cuatro historias de clientes reales de Cloudflare que afrontaron sus retos de gestión de bots con cuatro estrategias diferentes utilizando los productos de Cloudflare.

Bloquear los bots

Este enfoque requiere precaución, ya que muchos procesos comerciales legítimos, como la indexación de motores de búsqueda, requieren que los bots puedan acceder a los recursos de la empresa.

Bloquear los bots		
Desafíos	**Solución**	**Resultados**
Una empresa de juegos en línea notó un aumento importante en las quejas de los usuarios. Les estaban hackeando sus cuentas y robando la información de sus tarjetas de crédito. Actores maliciosos utilizaban bots automatizados para obtener credenciales de inicio de sesión por fuerza bruta, y accedían a cuentas de usuario y, en última instancia, las usurpaban.	El equipo de seguridad implementó el servicio de **la limitación de velocidad** junto con el de la **gestión de bots** avanzada para detectar múltiples intentos de inicio de sesión en un corto período de tiempo. Cuando se detectó un comportamiento inusual, la limitación de velocidad comenzó a bloquear automáticamente las solicitudes maliciosas. Desde que se implementó la función de la limitación de velocidad, la empresa de juegos en línea no ha sufrido un solo ataque de relleno de credenciales.	Todas las empresas deben equilibrar una seguridad rigurosa con una experiencia de usuario óptima. El conjunto de herramientas adecuado puede ayudar a detectar y prevenir el tráfico de bots maliciosos, y minimizar los falsos positivos y los obstáculos para los usuarios reales.

Reducir al enemigo

Esta técnica maximiza el tiempo de respuesta de todas las solicitudes de red sospechosas.

Reducir al enemigo		
Desafíos	**Solución**	**Resultados**
Una empresa de apuestas deportivas notó una reducción importante en las transacciones. Mientras analizaban el problema, identificaron actividad de bots maliciosos que estaban extrayendo las probabilidades de su sitio web y utilizaban esa información para obtener una ventaja competitiva.	La empresa no bloqueó los bots porque los agentes maliciosos evadirían el bloqueo. En cambio, disminuyeron la velocidad de la obtención de datos para las apuestas. Utilizaron la función **de anulación del encabezado** para identificar solicitudes sospechosas según el análisis de la **gestión de bots**, seguido de scripts de **Workers** para reaccionar a estos encabezados y disminuir las solicitudes.	Este método permitió a la empresa restablecer la actividad normal de los usuarios. Otros métodos incluyen el uso del desafío CAPTCHA para solicitudes de gran volumen o la modificación del marcado HTML a intervalos regulares. Estas acciones interrumpen el flujo de trabajo del bot, lo que complica la apropiación de contenidos consistente.

Engañar a los bots

Aunque muchas empresas implementan medidas para contrarrestar los bots, un atacante realmente decidido puede sortearlas. En cambio, algunas empresas deciden defenderse.

Engañar a los bots		
Desafíos	**Solución**	**Resultados**
Una empresa de apuestas deportivas intentó encontrar una solución para los bots que se apropiaban de las apuestas de su sitio web. Después de analizarlo detenidamente, decidieron implementar una solución alternativa mediante el uso de varios productos de Cloudflare que les permitiría proporcionar información aleatoria a los bots.	Cuando el sistema detectó que una solicitud fue generada por un bot malicioso, aceptó la solicitud y generó un nuevo flujo de trabajo: Solicitud → **WAF** (bot identificado) → **Gestión de bots** (clasificación de riesgo asignada) → **Workers** (generar datos aleatorios) → **Workers** (envío de datos aleatorios al bot)	El nuevo flujo de trabajo generó datos aleatorios nuevos que fueron devueltos a los bots maliciosos. Como resultado, los bots que venían a extraer apuestas e infligir daño se marchaban con algo inútil, lo que desalentaba cualquier abuso posterior.

Realizar un análisis dinámico

A medida que los bots se vuelven más sofisticados, las empresas necesitan recopilar datos sobre los bots y realizar análisis dinámicos antes de actuar. Estos objetivos pueden incluir la detección de registros erróneos, apuestas, reclamos de bonificación, etc. Para garantizar un análisis exhaustivo, los equipos de seguridad podrían necesitar combinar múltiples fuentes de datos de herramientas tanto internas como externas para analizar los parámetros del tráfico de bots.

Realizar un análisis dinámico		
Desafíos	**Solución**	**Resultados**
Una compañía de apuestas lanzó una campaña de marketing para atraer nuevos usuarios con recompensas al registrarse. Poco después del lanzamiento, detectaron que los bots estaban creando registros falsos. La empresa ya contaba con algunas herramientas de análisis internas, pero no ofrecían una visión completa del comportamiento de los bots.	El equipo implementó el servicio de la **gestión de bots** avanzada de Cloudflare con firmas JA3 para generar **registros sin procesar** de todo el tráfico de Internet que llega a la página de registro. Enriquecieron sus sistemas internos con puntuaciones de bots y firmas JA3, lo que les permitió identificar los bots de manera más precisa.	Tras un análisis exhaustivo, la empresa pudo cancelar los registros falsos y evitar inflar las estadísticas para los usuarios recién adquiridos. Introdujeron el análisis regular de análisis de bots mediante firmas JA3 en sus prácticas recomendadas.

Anticipate a los bots maliciosos

Gestión de bots de Cloudflare

Implementación simple
Sin configuraciones complejas ni mantenimiento.

Baja latencia
Latencia media de menos de 0,3 ms.

Análisis completo
Correlaciona los registros de tráfico con otras fuentes de datos, como los SIEM o las herramientas de BI.

Controles precisos
Personaliza las reglas, utiliza un generador visual de reglas o escribe tus propias reglas de coincidencia de patrones.

Detén los bots maliciosos antes de que afecten tu negocio

Los bots son cada vez más avanzados. Existen limitaciones inherentes en la detección y bloqueo de bots, ya que los métodos de ataque son cada vez más sofisticados. Las empresas actuales necesitan ajustar constantemente sus estrategias para hacer frente a la adaptación de los atacantes, y lograr el equilibrio adecuado entre una seguridad sólida y la minimización de la fricción del usuario.

Independientemente de la estrategia que decidas utilizar, asegúrate de que tu socio tenga un conjunto flexible de herramientas para gestionar los bots de forma eficaz. Para obtener más información sobre cómo Cloudflare puede ayudar con tus desafíos relacionados con bots, contáctanos para obtener una evaluación personalizada.

Información confiable

Cloudflare redirecciona mediante proxy casi el 20 % de todo el tráfico global de Internet, lo que proporciona una gran cantidad de información en tiempo real sobre el comportamiento de los bots maliciosos en toda la red de Cloudflare. Además, Cloudflare colabora con varios socios que comparten información sobre credenciales de inicio de sesión robadas, lo que facilita la detección de intentos de usurpación de cuentas antes de que resulten en una filtración.

Comienza tu recorrido hacia una red más rápida, confiable y segura

Solicitar una consulta

¿Aún tienes dudas?

Más información sobre **Cloudflare One**