INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Bot Manager

¿En quién confía? Y, lo que es igual de importante, ¿quién confía en usted? Debe confiar en que los consumidores, partners y bots que están al otro lado de las transacciones online son quienes dicen ser. Lamentablemente, muchos bots (que pueden representar hasta el 70 % del tráfico del sitio web) tratan de suplantar a usuarios legítimos, robar su propiedad intelectual y perjudicar sus operaciones. Akamai Bot Manager le ofrece visibilidad y control de los bots para ayudarle a proteger su negocio y garantizar, al mismo tiempo, la confianza de sus relaciones online.

Las empresas implementan cada vez más bots no maliciosos para automatizar las interacciones con los consumidores, partners, proveedores y terceros y aumentar, de este modo, su eficiencia online. Así, es necesario gestionar el impacto de esos bots en el rendimiento del sitio web y la experiencia del cliente.

Los estafadores y los delincuentes también automatizan cada vez más sus actividades y se valen de botnets para:

- Apropiarse del inventario antes de que los clientes puedan adquirirlo
- Lanzar ataques de Credential Stuffing
- Robar puntos de fidelidad y tarjetas regalo
- Aprovechar las vulnerabilidades de la lógica empresarial
- Atacar a empresas para ralentizar los sitios y aumentar los costes

Teniendo en cuenta la presencia de operadores de bots que pretenden perjudicar a su empresa y sus clientes, ¿cómo sabe que puede confiar en sus interacciones online? ¿Y cómo puede demostrar su fiabilidad a los demás?

Las inigualables funciones de detección y mitigación de Bot Manager le permiten llevar a cabo operaciones automáticas de forma más eficaz y segura, lo que refuerza su confianza y la de todo su entorno.

La confianza comienza con la gestión de bots de Akamai

Nuestra fortaleza global, tanto desde el punto de vista tecnológico como empresarial, hace que pueda confiar en Akamai. Prestamos servicio a más del 50 % de las empresas de la lista Global 500, contamos con más de 4150 puntos de presencia en más de 130 países y con unos ingresos anuales de más de 3600 millones de dólares. Aportamos toda esta capacidad a Bot Manager, innovando continuamente para garantizar que la solución no se quede anticuada y se mantenga un paso por delante de las tendencias de los bots y las técnicas de evasión.

VENTAJAS PARA SU EMPRESA

Mejore la confianza: La suya y la de sus clientes
Descubra qué interacciones son legítimas, reduzca los problemas de los usuarios y protéjalos de la actividad fraudulenta para fomentar la confianza entre los consumidores, los partners y usted.

Reduzca la carga de trabajo dedicada a la solución de problemas
Disminuya las pérdidas financieras y de recursos que suponen la comprobación de cuentas comprometidas, la sustitución de cuentas robadas, el tratamiento de las quejas de usuarios y otras consecuencias derivadas de los ataques de bots.

Mejore el control operativo
Mejore su eficiencia, reduzca los riesgos comerciales y financieros, controle los gastos de TI y gestione de forma estratégica los bots de los partners.

Tome mejores decisiones basadas en datos
Los análisis e informes detallados le ayudan a tomar decisiones creativas y eficaces sobre la trayectoria del cliente, la estrategia de seguridad, la tolerancia al riesgo y las operaciones de TI.

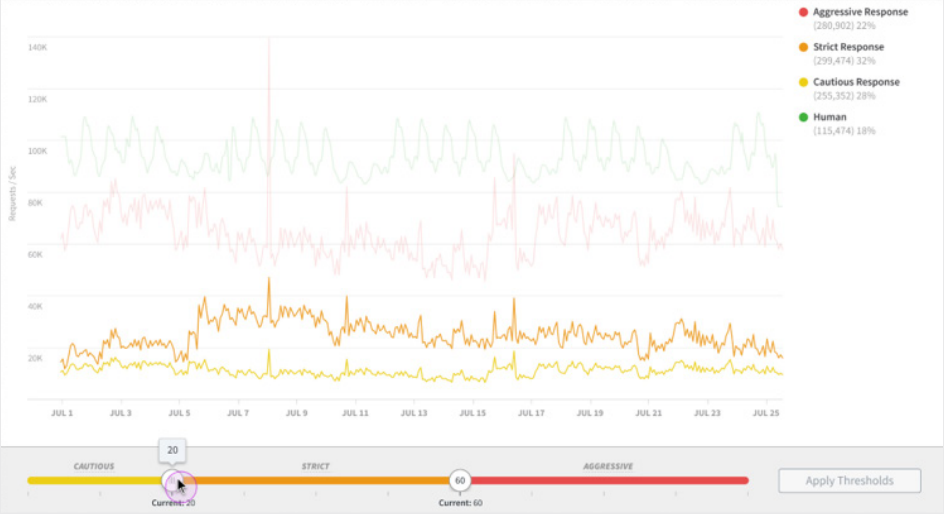
 | Asistencia | Publicado en octubre de 2023

Bot Manager utiliza tecnologías patentadas para detectar y mitigar los bots cuando establecen un contacto inicial, en lugar de permitirles acceder de inmediato al sitio web. Asimismo, no dejamos de trabajar para actualizar su protección a medida que las amenazas evolucionan. La información de nuestros investigadores especializados en inteligencia contra amenazas se incorpora automáticamente en las funciones de detección y análisis de Bot Manager, por lo que no es necesario solicitar ninguna actualización o mejora específica.

Bot Manager protege a su empresa independientemente del lugar en el que otros usuarios interactúen con usted, incluidos los terminales a través de la web, las aplicaciones móviles nativas y las API. Incluso le garantizamos la protección cuando una solicitud pasa de un dominio a otro. Si tiene varias marcas o empresas, Bot Manager sigue la solicitud inicial durante toda la interacción para que no haya brechas en la protección.

Marco de IA de Bot Manager

Bot Manager comienza con un marco de inteligencia artificial (IA) que funciona en línea en Akamai Connected Cloud. Esto permite a Bot Manager supervisar el tráfico en el Edge, donde un usuario se conecta por primera vez a una aplicación. De este modo, se obtienen datos precisos sobre patrones, tipos y volúmenes de tráfico. Akamai accede de media a 37 000 millones de solicitudes de bots al día en toda la red.



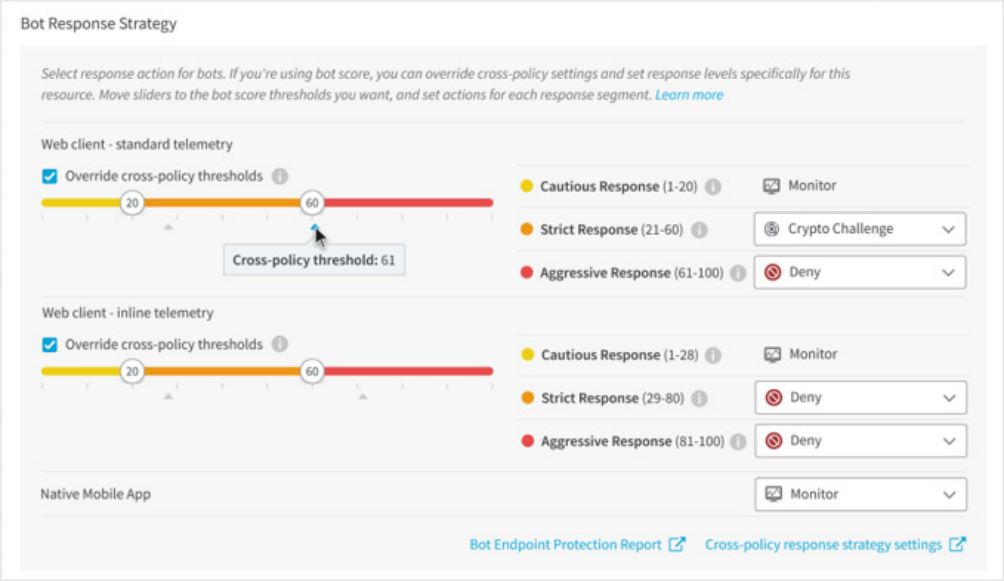
IA, aprendizaje automático e inteligencia contra amenazas

La recopilación de datos de "tráfico limpio" en una amplia distribución de tipos de datos y en grandes volúmenes permite perfeccionar nuestros algoritmos de aprendizaje automático (ML) para que sean más precisos. A través de la red de Akamai, supervisamos a diario el tráfico de 1300 millones de dispositivos únicos, con un tráfico récord de 164 Tbps. La visibilidad de estos datos permite a nuestros algoritmos aprender más y más rápido. Además, el equipo de Akamai, que cuenta con más de 400 investigadores especializados en amenazas, realiza un seguimiento constante de las tendencias en los patrones de ataque, la innovación tecnológica y las nuevas técnicas de evasión con el fin de mejorar nuestra capacidad de detección. Los investigadores especializados en amenazas de Akamai analizan cada día 662 TB de nuevos datos de ataque, frente a los 290 TB en 2021.

Además de las potentes técnicas de IA y ML de Akamai, ahora ofrecemos la posibilidad de crear modelos específicos para cada cliente. Estos modelos de aprendizaje profundo analizan los ataques más sofisticados que observamos en los sitios web de grandes marcas que suelen estar en el punto de mira. A continuación, el modelo convierte el aprendizaje en algoritmos avanzados para implementar mecanismos de mitigación contra nuevos tipos de ataques en cuestión de minutos, en lugar de los días o incluso semanas que requieren otros métodos.

Bot Score: evalúe cada bot con cada detección

Bot Score combina de manera holística todos los activadores de detección para identificar bots sofisticados y ofrecerle una evaluación más precisa de cada solicitud, lo que optimiza la eficacia de detección general del sistema, todo ello sin que aumente la latencia. Además, le permite definir una estrategia de respuesta basada en las puntuaciones obtenidas.



Desafíos innovadores

Al combinar la función Bot Score de Bot Manager con desafíos vanguardistas, disfrutará de la comodidad de tomar medidas de forma automática mediante acciones de respuesta y umbrales predefinidos. Transfiera la "carga de la prueba" de los usuarios legítimos a los bots gracias a nuestros desafíos invisibles para humanos. El desafío criptográfico obliga a los bots a dedicar ciclos de CPU a resolver rompecabezas criptográficos que requieren un mínimo de tiempo, lo que decelera los ataques de los bots más sofisticados y aumenta los costes para los autores de los ataques. El desafío intercalado requiere que los clientes demuestren que admiten el almacenamiento de cookies y la ejecución de JavaScript. En caso contrario, Bot Manager aplica una penalización de tiempo además de la acción de respuesta que elija como medida de mitigación.

Protección contra ataques por efecto de red

Garantizamos la protección de algunas de las empresas más grandes y conocidas del mundo, que son a menudo blanco de los operadores de bots más avanzados. Si se detecta un nuevo bot en un cliente, los datos del bot se añaden a la biblioteca de bots y a nuestro exclusivo algoritmo, que envía los datos del bot a todos los clientes en cuestión de minutos. Este efecto de red no solo permite a los clientes gestionar los bots de forma eficaz, sino que también nos permite evitar de forma anticipada que algunos bots ataquen a los demás.

Implementación rápida y simplificada

La arquitectura en línea de Bot Manager le permite implementarlo de forma rápida y sencilla. Además, es eficaz desde el momento en que se activa, ya que detecta los bots en tiempo real sin que se produzca ninguna latencia ni afecte al rendimiento del sitio web o de la red. Bot Manager también se adapta a sus necesidades, gracias a la capacidad masiva de la red de Akamai. ¿Cuál es la capacidad de nuestra red? El tráfico en nuestra red supera los 100 Tbps día tras día. El pico máximo histórico, del 14 de diciembre de 2022, fue de 261,21 Tbps.

Funciones clave

Directorios de bots conocidos: Bot Manager responde automáticamente a los bots conocidos, y actualizamos continuamente nuestro directorio actual que consta de 1750 bots conocidos.

Detecciones sofisticadas y dinámicas de bots: Bot Manager detecta con precisión los bots desconocidos desde la primera interacción gracias a una serie de modelos y técnicas de inteligencia artificial y aprendizaje automático. Estas técnicas incluyen el análisis del comportamiento, la huella digital y la detección automática del navegador, la detección de anomalías de HTTP e índices elevados de solicitudes, entre otras. La telemetría y la ocultación dinámica de código de Bot Manager protegen contra la ingeniería inversa, con lo que se consigue que Bot Manager siga resultando muy eficaz con el tiempo.

Modelo de puntuación: el modelo Bot Score evalúa cada solicitud con cada detección de Bot Manager Premier. Después, calcula la probabilidad de que la solicitud provenga de un bot y otorga una puntuación que abarca de 0 (sin duda un humano) a 100 (sin duda un bot).

Detección de suplantación del navegador: los operadores de bots a menudo intentan suplantar ciertos navegadores para evitar su detección. Hemos conseguido que nuestra detección de suplantación de navegadores sea muy precisa sin necesidad de ajustarla habitualmente, por lo que los clientes reciben menos falsos negativos que con otros métodos de detección.

Configuración personalizada por terminal: la función Bot Score le permite establecer respuestas estratégicas distintas para cada terminal. Por ejemplo, puede aplicar la respuesta Cautelosa (observar/supervisar) a los bots con puntuaciones de 35 o menos en su página de búsqueda, pero reducir el umbral a 20 para las solicitudes en su página de inicio de sesión.

Simulador de optimización de respuesta: puede optimizar sus respuestas estratégicas según el terminal y la tolerancia al riesgo de su organización. Bot Score le permite realizar simulaciones de optimización antes de aplicar los ajustes, de modo que pueda ver el impacto de los cambios en los umbrales en función del tráfico que ha tenido en el pasado.

Optimización automática: reduzca la necesidad de intervención humana durante la optimización, incluso a medida que los bots evolucionan. Bot Manager memoriza los patrones de tráfico habituales de sus sitios web y optimiza automáticamente las detecciones en función de sus patrones únicos para evitar posibles errores al clasificar las solicitudes.

Acciones de respuesta matizadas: mejore la mitigación de bots con acciones que van más allá de bloquear y permitir, como ofrecer un contenido alternativo, presentar un desafío, ralentizar y mucho más.

Análisis y elaboración de informes detallados: tome decisiones basadas en datos fiables con los informes históricos y en tiempo real de Bot Manager. Obtenga visibilidad de las tendencias globales y análisis detallados de bots individuales u otros segmentos del tráfico de bots. También puede comparar el tráfico de bots con otros usuarios del sector y todos los clientes de Akamai.

Servicio de seguridad gestionado (opcional): optimice Bot Manager sin sobrecargar a su equipo interno con ayuda del servicio de seguridad gestionado, Managed Security Service, de Akamai. Los expertos de Akamai monitorizan y proporcionan recomendaciones de respuesta proactivas, además de ofrecer asistencia en situaciones de emergencia en caso de detectar eventos que afecten a la seguridad.

Gestión de bots con reconocimiento del riesgo

- Respalde los objetivos corporativos alineando su respuesta a bots con la tolerancia al riesgo de su empresa
- Modifique los umbrales de puntuación para que se adapten a objetivos a largo plazo y a eventos concretos como ofertas especiales de un solo día
- Elija las respuestas estratégicas según el terminal. Por ejemplo, puede aplicar acciones agresivas cuando se detecten puntuaciones de riesgo más bajas en terminales de gran importancia

Póngase en contacto con su representante de Akamai o visite Akamai.com para obtener más información.