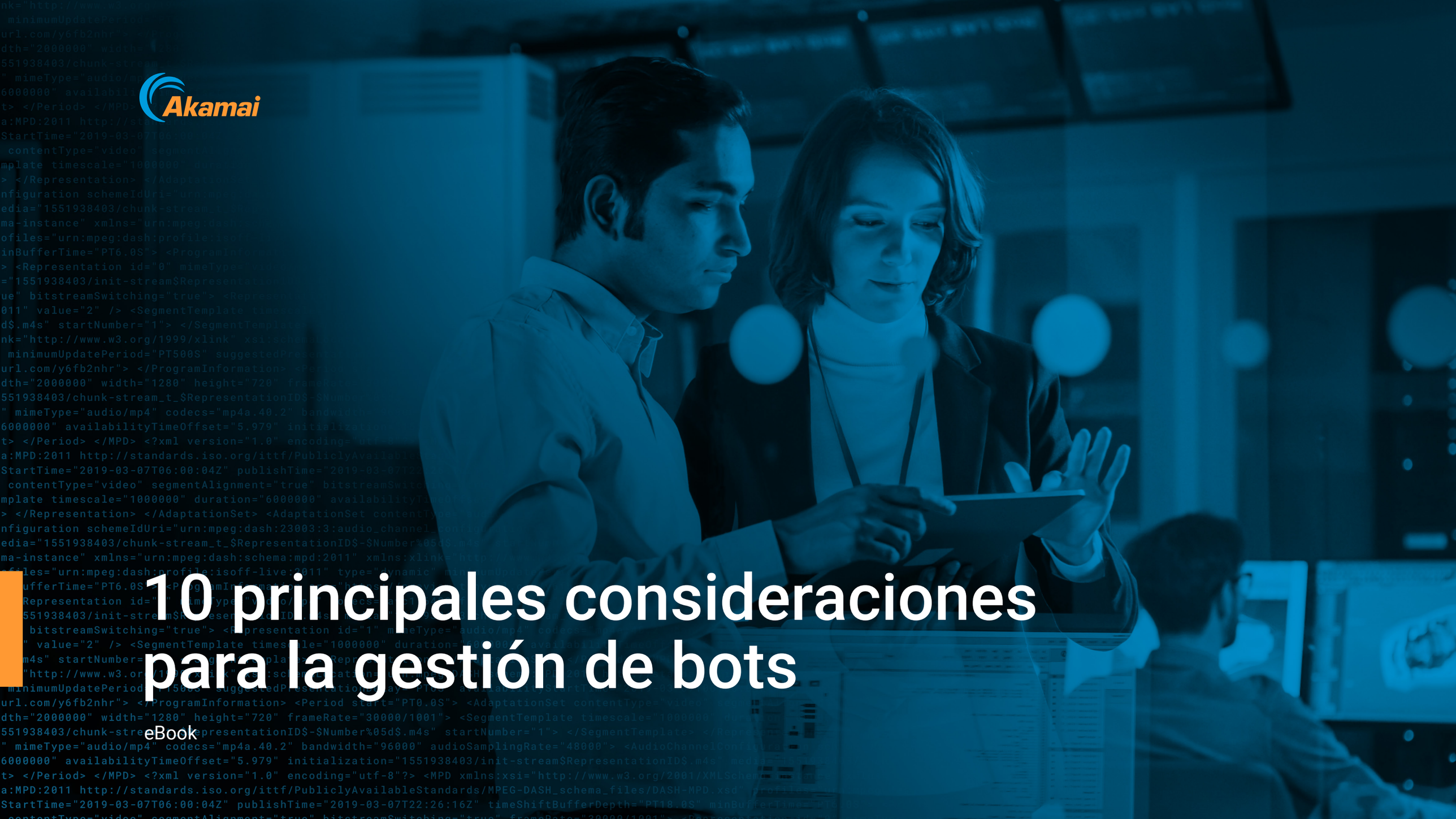

# 10 principales consideraciones para la gestión de bots

eBook

## TABLA DE CONTENIDO

# Introducción

¿Se plantea la magnitud que ha adquirido el problema de los bots? Intente conseguir una entrada para ver a Taylor Swift o las nuevas Air Jordan. Y aquí hablamos simplemente de eventos muy esperados. Los bots son cada vez más omnipresentes y tienen un efecto nefasto en todos los sectores.

Lo peor para quienes buscan respuestas es que las reglas del juego de la gestión de bots han cambiado. En realidad, siempre han estado sometidas a un cambio constante. La gestión de bots se suele describir como una carrera armamentista, o un juego del gato y el ratón, en el que las empresas levantan defensas y los creadores de bots buscan continuamente formas de eludirlas. Sin embargo, ahora no son solo los propios bots los que están evolucionando. El entorno que los rodea también está evolucionando. Por ejemplo, las empresas ya no tratan solo con actores individuales, ni siquiera con grupos coordinados. Ahora se puede alquilar un bot para la semana, como haría con un Airbnb. Del mismo modo, las soluciones no pueden simplemente clasificar los bots en buenos y malos, ya que, actualmente, hay demasiadas zonas intermedias.

Esta evolución de los bots y del entorno que los rodea ha dificultado más que nunca la selección de un software para su gestión. No solo es necesario saber qué métodos han funcionado para luchar contra los bots del pasado, sino también cuáles serán eficaces contra los bots actuales y futuros.

Esta guía describe algunas de las consideraciones clave que deben tener en cuenta los compradores a la hora de elegir un software de gestión de bots. Le resultará útil para separar el grano de la paja y tomar una decisión de compra fundamentada.

# 1 Competencia sofisticada

Por definición, las soluciones de gestión de bots detectan bots. Es decir, buscan señales de automatización y otros indicadores de que el solicitante no es un ser humano. Sin embargo, a medida que los bots han ido evolucionando y se han ido volviendo más sofisticados, también se han especializado más. Los bots actuales están diseñados para fines específicos, como extraer contenido de los sitios, acaparar existencias durante eventos muy esperados, así como Credential Stuffing para apropiarse de las cuentas de sus clientes, entre otros casos de uso. Y, a menudo, las detecciones de un tipo de bot especializado no permiten detectar los demás tipos. Necesita saber si el proveedor es capaz de bloquear a los bots específicos a los que se enfrenta y no solo a los bots básicos generales.

**Aspectos clave:**

- ¿Dispone el proveedor de mecanismos de detección de bots especializados en casos de uso empresariales?
- ¿Puede demostrar el proveedor su competencia en el problema específico de bots al que se enfrenta?
- ¿Cuántos de los otros clientes del proveedor tienen los mismos problemas? ¿Se podrá beneficiar usted de lo que el proveedor ha aprendido de esos clientes?
- ¿Ofrece el proveedor informes, servicios u otras funciones para dotarle de aún más recursos en su lucha contra los ataques de bots especializados?

# 2 Inteligencia

La eficacia de una solución de gestión de bots se mide por su capacidad para reconocer las características de los bots que supervisa. Aunque algunos proveedores afirman detectar el 99,9 % de los bots, resulta imposible medir objetivamente la eficacia. Los bots cambian constantemente, por lo que lo que detectó ayer probablemente hoy ya haya aprendido a evadir esa detección. Un criterio más idóneo para evaluar las herramientas de gestión de bots es cómo actualiza el proveedor sus funciones de detección de bots. Es necesario contar con una solución capaz de detectar los bots más sofisticados (no solo los sospechosos habituales) y de extraer información del conjunto de datos más grande. Tenga en cuenta que muchas herramientas de inteligencia artificial (IA) y de aprendizaje automático (ML) son de código abierto, por lo que la cantidad de datos, la limpieza de estos y la velocidad con la que la solución envía los datos a los algoritmos son factores cuya importancia no se tiene suficientemente en cuenta a la hora de evaluar la función de IA/ML de una solución.
La información debe incluir indicadores de confianza y puntuaciones de riesgo en todos los inicios de sesión y dominios. Además, para ser eficaces, las soluciones deben adoptar un enfoque heterogéneo en la detección de bots y utilizar los métodos más recientes.

**Aspectos clave:**

- Solicite más información sobre cómo el proveedor actualiza sus funciones de detección de bots. Los proveedores con clientes importantes que resultan atractivos para los atacantes tendrán más experiencia y contarán con conjuntos de datos más completos en los que apoyarse para desarrollar sus competencias, incluidas las señales de riesgo y confianza que evaluar, más mecanismos para la detección de anomalías en dispositivos, entre otras. La falta de transparencia debería ser una señal de alerta.
- ¿Utiliza el proveedor IA/ML para mejorar la solución? ¿Qué nivel de sofisticación tienen esos modelos? E igual de importante: ¿Cuántos datos introduce el proveedor en esos modelos? Sin duda, los atacantes utilizan la IA. Usted también debería usarla.
- Sin embargo, la IA no es suficiente. ¿Cuenta el proveedor con un equipo de expertos cualificados, como investigadores de seguridad y analistas de inteligencia sobre amenazas, que buscan constantemente nuevas técnicas de ataque y que supervisan las comunidades de hackers para asegurarse de que usted esté siempre un paso por delante?

# 3 Protección sólida

Los bots más sofisticados no desaparecen de forma permanente por mucho que los bloquee. Vuelven una y otra vez, mutando constantemente en un intento por evitar los mecanismos de detección. Muchas soluciones de gestión de bots pueden detectarlos (o al menos, algunos de ellos) inicialmente, pero después pierden efectividad cuando los bots empiezan a mutar. Akamai ha sido testigo de cómo los bots mutan en cuestión de horas. Los ciclos de desarrollo tradicionales son demasiado lentos y no son capaces de seguirles el paso. Asegúrese de que la solución por la que opte aprende y evoluciona con el tiempo, preferiblemente mediante el aprendizaje automático. La solución debería incluir defensas preventivas que dificulten la tarea de los atacantes de obtener información que les sirva para eludir sus defensas.

**Aspectos clave:**

- Busque una solución que aplique las tecnologías de detección de bots más sofisticadas (como el análisis del comportamiento de los usuarios y modelos de aprendizaje específicos para cada cliente), puesto que serán eficaces durante más tiempo, pese a la mutación de los bots.
- Descubra si la solución incluye tácticas defensivas como la ofuscación de código JavaScript, que dificulta a los atacantes aplicar ingeniería inversa a los bots para burlar sus defensas.
- Solicite pruebas o referencias a otros clientes que ya hayan implantado la solución para saber si ha mantenido la eficacia con el paso del tiempo.

# 4 Falsos positivos y falsos negativos

Cuando una solución de gestión de bots muestra que bloqueó un bot, ¿cómo sabe que el sistema realmente no bloqueó a un usuario legítimo? Muchos proveedores se toman a la ligera los falsos positivos. Si no cuentan con una solución que puntúe los bots en cada detección, es posible que no puedan detectar los bots intermedios, con decisiones binarias de tipo sí/no. Y, a menudo, a esos proveedores les gusta mostrar a los clientes que han bloqueado muchos "bots", incluso aunque su tasa de falsos positivos sea alta, lo que significa que están deteniendo bots, pero también tráfico válido: seres humanos o bots "buenos" que son valiosos para su empresa. Por otro lado, una tasa baja de falsos negativos suena muy bien hasta que se da cuenta de que esa tasa se debe a que el proveedor ha tenido que reducir la eficacia general de la solución para asegurarse de no bloquear a los usuarios humanos y, a continuación, acaba dejando pasar a bots que no debería. Usted quiere bloquear a los bots maliciosos sin que esto afecte a la actividad de su empresa, pero tampoco desea bajar su nivel de protección. Debe poder confiar en que al proveedor que le presta sus servicios le preocupan la precisión y el efecto de los falsos positivos y los falsos negativos.

**Aspectos clave:**

- ¿El proveedor delega en usted la tarea de gestionar los falsos positivos/negativos o invierte en funciones y servicios para colaborar con usted?
- ¿La solución aprende de los patrones de tráfico de los distintos sitios y se ajusta automáticamente para reducir la carga de trabajo de su equipo?
- ¿Sugiere el proveedor utilizar un CAPTCHA en lugar de otras acciones de desafío? Esta sugerencia suele ser muy reveladora. Los usuarios los odian, pero para los proveedores es más fácil ofrecer un CAPTCHA que ajustar sus reglas para minimizar los falsos positivos.
- ¿Tiene visibilidad que le permita saber por qué se ha marcado una solicitud como procedente de un bot? ¿O la solución es una caja negra? Lo ideal sería tener capacidad para verificar las acciones realizadas con una visibilidad detallada de las solicitudes y la posibilidad de visualizar los cambios de configuración antes de llevarlos a la fase de producción.

# 5 Acciones flexibles

Es tentador pensar que solo tiene que preocuparse por bloquear los bots malos y dejar pasar a los buenos. Pero el entorno se ha vuelto mucho más complejo que eso. Muchos operadores de bots han aprendido a reducir sus señales de riesgo lo suficiente como para poner sus bots en una zona intermedia, conscientes de que la mayoría de las organizaciones preferirían arriesgarse a dejar entrar un bot malicioso que bloquear a un usuario legítimo. Su solución debe proporcionar un conjunto de acciones sofisticadas para que pueda no solo bloquear o autorizar, sino también incluir acciones de desafío, como desafíos criptográficos y autenticación multifactorial (MFA) adaptativa. Además, su solución también debe incluir acciones para gestionar otros tipos de situaciones, como los bots buenos. Es posible que desee ralentizar los bots de sus partners durante las horas de tráfico intenso y dejarlos pasar de forma inmediata durante las horas de menor actividad. También puede elegir diferentes acciones para los bots de la misma categoría conocida; por ejemplo, si es retailer, puede dejar que los bots de cupones más conocidos visiten su sitio y bloquear aquellos con los que no desea trabajar. Necesita disponer de flexibilidad para aplicar diferentes acciones según el tipo de bot y el impacto que tenga en la empresa y en la TI, sobre todo cuando este varía según la ubicación, la hora del día o la estacionalidad. Además, necesitará una solución que no solo bloquee todos los bots (y, al hacerlo, les enseñe a cambiar las tácticas de evasión), sino que cree obstáculos, lo que lo hará que sea más difícil y más caro para los atacantes.

**Aspectos clave:**

- ¿La solución le permite crear diversas categorías en función del tipo de bot, o solo distingue entre buenos y malos? ¿Puede también crear distintas acciones para bots de la misma categoría, como motores de búsqueda o agregadores financieros?
- ¿Qué tipos de acciones condicionales admite la solución? ¿Acaso ofrece acciones avanzadas, como ralentizar o proporcionar contenido alternativo, para modelar mejor el tráfico? ¿Incluye acciones como un desafío criptográfico?
- ¿Qué grado de flexibilidad ofrece la solución a la hora de gestionar los diferentes tipos de bots que se presentan? ¿Actúa simplemente como un mero martillo o puede aplicar acciones con precisión quirúrgica en función de la hora del día, el porcentaje de tráfico o la URL?
- ¿Puede la solución introducir problemas de alto consumo de recursos que aumenten el coste para los operadores de bots y ralenticen los ataques de gran volumen de solicitudes más allá de un error de acceso 403?

# 6 Implantación

Cuando se trata de cualquier solución de gestión de bots, el tiempo que se tarda en lanzar la solución y la rapidez con la que la pueda modificar deben ser factores clave. Los compradores deben tener cuidado con cualquier solución que les exija modificar sus aplicaciones existentes o que afecte al rendimiento de las mismas. Los retrasos en la implantación pueden resultar costosos y, si debe hacer cambios en las aplicaciones cada vez que las circunstancias de la empresa lo requieran, como las ventas relámpago, eso va a exigir más recursos.

**Aspectos clave:**

- ¿Funciona la solución en tiempo real sin que el rendimiento de sus aplicaciones existentes se vea afectado?
- ¿Le exige realizar cambios en sus aplicaciones existentes?
- ¿Se puede ampliar o reducir su escala para adaptarse a eventos imprevistos como ataques volumétricos o eventos previstos como ventas relámpago?

# 7 Visibilidad y generación de informes

Cualquier solución de gestión de bots puede mostrarle estadísticas generales sobre el tráfico de bots, pero se necesita algo más que eso. Para planificaciones de infraestructura o facilitar informes a sus superiores, las estadísticas generales son excelentes, pero no muestran suficientes detalles para analizar el tráfico de bots. Tampoco le aportan las pruebas que necesita para confirmar que la solución está tomando las medidas adecuadas. Con una solución que podría bloquear a sus usuarios, lo menos recomendable es una caja negra. Necesita informes detallados para gestionar su negocio y que pueda comprender mejor cómo los cambios en los umbrales de riesgo afectan al rendimiento.

**Aspectos clave:**

- ¿La solución ofrece funciones de generación de informes que aporten detalles sobre bots, botnets y características de bots específicos? ¿Puede informar sobre distintos segmentos de puntuación, qué bots atacan a qué terminales y mostrar qué medidas se han adoptado?
- ¿Es posible investigar picos de tráfico y consultar cada una de las solicitudes? A veces lo más útil es ver los detalles de la solicitud para decidir qué hacer.
- ¿Puede la solución mostrarle una comparación entre su tráfico de bots y el de otros del sector?
- ¿Cómo se integran las funciones de generación de informes con las de otras soluciones de seguridad? ¿Puede analizar el tráfico de manera global o hay vistas independientes?

# 8 Protección de las API

Independientemente del proveedor o de la solución, las tecnologías de detección de bots más sofisticadas de hoy en día se basan en la inyección de código de JavaScript y el análisis de la respuesta del cliente. Pero, ¿qué hacer con las API cuando los clientes basados en API no responden a JavaScript? Si necesita dejar las API expuestas para admitir a terceros o aplicaciones móviles, debe contar con una solución que las proteja de la misma manera que lo hace con sus páginas web. De lo contrario, sus bots (y los problemas relacionados) no harán más que migrar de sus páginas web a sus API.

**Aspectos clave:**

- ¿Qué tipo de protección para API ofrece el proveedor? ¿Se trata solo de la gestión de la cuota y la limitación de velocidad?
- Aspire a una capacidad móvil capaz de incorporar la detección de bots más sofisticada del proveedor a sus aplicaciones móviles.
- Aunque no siempre es tan eficaz como otras detecciones activas, un enfoque basado en la reputación puede ser una buena opción para proteger las API compatibles con terceros que no tengan acceso a una capacidad móvil, como un SDK.

# 9 ¿Sitio o página?

Si su sitio web tiene más de una página, es probable que tenga diversos problemas de bots que afecten a las diferentes partes del sitio. El scraping de precios puede tener un gran impacto en las páginas de sus productos. El scraping de su contenido puede socavar su contenido digital de valor añadido. Mientras tanto, siguen produciéndose ataques de abuso de credenciales a las páginas de inicio de sesión. Sin embargo, cuando se trata de soluciones de gestión de bots, algunas están diseñadas únicamente para resolver un solo problema. Asegúrese de que su solución de gestión puede ayudarle a abordar todos sus problemas de bots, independientemente de que afecten a todo el sitio o solo a determinadas páginas.

**Aspectos clave:**

- ¿Qué abarca la solución? ¿Ciertas páginas o todo el sitio web?
  ¿Cómo se implanta? ¿Delante de las páginas por separado o de todo el sitio web?
- ¿Puede ayudarle a abordar todos sus problemas de bots, ya se trate de abuso de credenciales, scraping web o agregación de contenidos?

# 10 Servicios gestionados

Es preciso gestionar los bots para controlar sus efectos sobre usted y su negocio, pero esta gestión no es fácil. Y aunque cuente con personal competente en su empresa, a veces necesita ayuda extra: necesita la ayuda de expertos en problemas relacionados con los bots. Además, cada vez es más difícil dotar de personal estos puestos. ¿Qué sucede cuando parte de su talento deja la empresa? Cualquiera puede analizar una solicitud HTTP y crear una firma para bloquear el tráfico, pero así no se soluciona el problema. Lo que necesita es alguien que pueda establecer una correlación entre sus problemas principales y el tipo de bots, y diseñar e implementar una estrategia capaz de resolverlos.

**Aspectos clave:**

- ¿Dispone en su empresa de los conocimientos específicos en materia de bots para sacar el máximo partido de cualquier solución?
- ¿El proveedor de gestión de bots le ofrece servicios profesionales o solo vende productos?
- ¿Puede acceder a la supervisión proactiva y a recursos expertos complementarios en caso de emergencia en cualquier momento?

# Sea proactivo, no reactivo

Es mejor invertir en la gestión de bots antes de que los bots se conviertan en un problema y antes de que la siguiente ola de evolución convierta las defensas existentes en una mala imitación de sus homólogas anteriores. Tenga en cuenta estas consideraciones cuando analice sus opciones. Akamai Bot Manager puede proporcionarle las garantías que necesita. Para obtener más información, solicite una guía personalizada de un ataque simulado.

**Más información**