LIBRO ELECTRÓNICO

# 10 principales consideraciones para la GESTIÓN DE BOTS

Para más información, visita: https://www.dimtec.com
Contactáme: Diana Pardo Pardo, dpardo@dimtec.com

Akamai

# ¿Cuál es la solución de gestión de bots más adecuada?

Si eligiera un sitio web al azar, se sorprendería. Probablemente, descubriría que, según un estudio interno de Akamai, los robots web automatizados (bots) generan entre un 30 y un 70 % del tráfico total de los sitios web actuales. Esta sencilla estadística oculta una realidad compleja: identificar el tráfico procedente de bots es una cosa, pero saber qué medidas tomar al respecto (y llevarlas a cabo) es algo mucho más complicado.

El mercado de la gestión de bots está en constante evolución e incluye muchos proveedores de diferentes tamaños, que tienen diversos conocimientos y competencias. No obstante, si en algo se parecen es en el marketing: todos dicen que tienen la solución a sus problemas. Debe ver más allá del marketing y centrarse en la capacidad real. Es decir, ir al grano: los resultados. Debe aprender a evaluar las soluciones de gestión de bots y comprender qué implican las diferencias.

**Este es el propósito de este libro electrónico. Le invitamos a seguir leyendo.**



More Information, visit: https://www.dimtec.com
Contact me: Diana Pardo Pardo, dpardo@dimtec.com

# Elección de la solución adecuada

Al igual que con cualquier otra herramienta, una solución de gestión de bots adecuada es aquella que cumple su cometido y contribuye a cumplir los objetivos. Así, podrá ***satisfacer las necesidades de su empresa además de controlar todo el contenido malicioso*** que le quita el sueño. Pero, ¿cómo averiguar si la solución le ofrecerá todas estas prestaciones sin apostar todo su presupuesto y uno o más años de su vida para comprobarlo? Le ofrecemos una lista de los 10 factores principales que debe tener en cuenta al elegir una solución de gestión de bots.



**Debe aprender a evaluar las soluciones de gestión de bots y comprender qué implican las diferencias.**


Para más información, visita: https://www.dimtec.com
Contactáme: Diana Pardo Pardo, dpardo@dimtec.com

# 1. Eficacia

Hay proveedores que afirman ser capaces de detectar el 99,9 % de los bots, lo cual le hará pensar que se les da muy bien el marketing. Aunque, solo con reflexionar un segundo, es un argumento que cae por su propio peso. ***¿Cómo puede afirmar un proveedor que detecta el 99,9 % de los bots si no detecta con certeza el 100 %?*** Y si sabe con certeza cuáles son el 100 % de los bots, ¿por qué detectar solo el 99,9 %?

Todas las soluciones pueden detectar los bots, la cuestión es cuántos. El problema es que los bots cambian constantemente, así que es imposible calcular la eficacia de forma objetiva. No obstante, puede calcular la sofisticación de los bots que detecta. Equípese con buenos conocimientos acerca del panorama de bots, de las tecnologías de detección y de las diferencias entre ellas. Asegúrese de que la solución que está evaluando pueda detectar los bots más sofisticados con los que se pueda encontrar.

**Aspectos clave:**

- Para saber qué expectativas crearse en general, investigue qué tecnologías de detección de bots aplica la solución y qué grado de sofisticación poseen.
- No todas las implantaciones de una tecnología son iguales. Compare varias soluciones presentadas como similares para ver cómo funcionan en su entorno.
- Póngase en la piel de un atacante: ¿existe alguna herramienta con la que superar los mecanismos de detección de la solución? Si es así, quizás no sea la más adecuada.

**Asegúrese de que la solución que está evaluando pueda detectar los bots más sofisticados con los que se pueda encontrar.**

# 2. Protección sólida

Los bots no se van por mucho que los bloquee. Vuelven una y otra vez, a la vez que mutan en un intento por evitar los mecanismos de detección. Muchas soluciones de gestión de bots pueden detectarlos (al menos, algunos) inicialmente, pero después los pierden de vista cuando estos empiezan a mutar. ***Asegúrese de que la solución que elige puede aprender y evolucionar con el tiempo*** para ayudarle en todo momento a resolver sus problemas a largo plazo.

**Aspectos clave:**

- Busque una solución que aplique las tecnologías de detección de bots más sofisticadas (como el análisis del comportamiento de los usuarios), puesto que serán eficaces durante más tiempo, pese a la mutación de los bots.

- 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.

**Muchas soluciones de gestión de bots pueden detectarlos inicialmente, pero después los pierden de vista cuando estos empiezan a mutar.**

# 3. Falsos positivos

Cuando una solución de gestión de bots muestra que bloqueó un bot, ***¿cómo sabe que el sistema realmente bloqueó un bot y no a un usuario legítimo?*** Muchos proveedores se toman a la ligera los falsos positivos. Para algunos, mostrarle al cliente que han bloqueado muchos "bots" es más importante que asegurarse de que no bloquean tráfico válido (personas o bots "buenos" valiosos para su empresa). No obstante, lo que necesita es resolver el problema de los bots sin que ello afecte negativamente a su negocio. Debe poder confiar en que al proveedor que le presta sus servicios le preocupan la precisión y el efecto de los falsos positivos.

**Aspectos clave:**

- ¿El proveedor elude la tarea de ajustar la configuración para evitar falsos positivos o se preocupa por minimizarlos él mismo?
- ¿El proveedor le ha sugerido utilizar un CAPTCHA? 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? Busque aquella que le permita verificar las acciones que se han realizado y ofrezca una visibilidad precisa de las solicitudes.

**Lo que necesita es resolver el problema de los bots sin que ello afecte negativamente a su negocio.**

# 4. Acciones flexibles

La mayoría de las soluciones de gestión de bots optan por un enfoque de protección ante el problema. Dan por sentado que todos los bots son maliciosos (y que, por tanto, se deben bloquear), excepto algunos específicos que se sabe que son inocuos (porque se incluyen específicamente en una lista de autorización). Sin embargo, ¿qué ocurre con los bots "buenos" que también aniquilan el rendimiento de los sitios web? ¿Y con los servicios emergentes para el consumidor que permiten a los clientes comunicarse con usted de nuevas formas? El hecho es que existe una amplia gama de bots cuyo impacto no suele quedar claro. De hecho, incluso el mismo bot "bueno" puede afectar de forma diferente a su negocio según la hora del día en que funcione.

***Necesita disponer de flexibilidad para aplicar diferentes acciones según el tipo de bot y el impacto que tenga en el negocio y en la TI***, sobre todo cuando este varía según la ubicación, la hora del día o la estacionalidad.

**Aspectos clave:**

- ¿La solución le permite crear diversas categorías en función del tipo de bot, o solo distingue entre buenos y malos?
- ¿Qué tipos de acciones permite realizar la solución? ¿Solo bloquear y aplicar un CAPTCHA? ¿O acaso ofrece acciones avanzadas, como ralentizar o proporcionar contenido alternativo para modelar mejor el tráfico?
- ¿Qué grado de flexibilidad ofrece la solución a la hora de gestionar los diferentes tipos de bots que se presentan? ¿Actúa 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?

**Existe una amplia gama de bots cuyo impacto no suele quedar claro.**

# 5. Visibilidad e 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. Cuando se trata de una solución que podría bloquear a sus usuarios, lo menos recomendable es una caja negra. La solución que elija debe ofrecerle los informes detallados necesarios para ayudar a su empresa y acelerar la recopilación de información.

**Aspectos clave:**

- ¿La solución ofrece funciones de generación de informes que aporten detalles sobre bots, botnets y características de bots específicos?
- ¿Es posible investigar un pico 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.
- ¿Cómo se integran las funciones de generación de informes con las de otras soluciones de seguridad? ¿Puede analizar el tráfico de manera global o cada solución es independiente?

**Cuando se trata de una solución que podría bloquear a sus usuarios, lo menos recomendable es una caja negra.**

# 6. 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 un kit de desarrollo de software (SDK) 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 un SDK.

**Si no protege las API, sus bots no harán más que migrar de sus páginas web a sus API.**

# 7. ¿In situ o en la nube?

Hay debates eternos: ¿el huevo o la gallina? ¿"Star Trek" o "Star Wars"? ¿In situ o en la nube? Existe una amplia gama de soluciones de gestión de bots. Algunos proveedores ofrecen soluciones in situ. Otros, las estructuran como soluciones basadas en la nube. Debe averiguar qué es lo que más le conviene, pero ***también evaluar cómo encajará la solución en el resto de su infraestructura web.*** ¿Dispone de servidores web in situ o en la nube? ¿Tiene uno o varios centros de datos? ¿Usa una red de distribución de contenido (CDN)? Todas estas variables influirán en su elección.

**Aspectos clave:**

- ¿Cuáles son sus requisitos de escalabilidad? Averigüe si una solución implantada en las instalaciones podría resistir picos de tráfico o el ritmo de crecimiento previsto.
- ¿Necesita aligerar el tráfico en el origen? Para usar una solución in situ, es necesario hacer llegar el tráfico hasta su centro de datos, mientras que una CDN puede gestionar el tráfico de bots en la nube.
- Si utiliza una CDN, ¿qué ocurriría si implantara otro servicio basado en la nube delante de su sitio web?

**Una solución debe proteger sus aplicaciones, sin importar dónde se ubican.**

# 8. Desarrollo general

¿Es su sitio o aplicación web el alma de su negocio? ¿Son los requisitos en cuestión de tiempo de actividad tan rigurosos que solo es posible hacer cambios en la aplicación en los intervalos de tiempo predefinidos? Si la respuesta es sí, ***debe determinar qué cambios impondrá la solución propuesta.*** Algunos proveedores necesitan que cambie la aplicación para que efectúe una llamada de API a la solución. Otros necesitarán que codifique su JavaScript en cualquier página que desee proteger. Eso significa que quizás tenga que añadir la solución en el ciclo de vida de su aplicación. Y no solo eso. Siempre que el proveedor cambie de solución o el código JavaScript, quizás tenga que modificar también su aplicación.

**Aspectos clave:**

- ¿Cómo se implanta la solución? ¿Se trata de una solución en línea que se sitúa por delante de su aplicación? ¿O se ubica fuera de banda?
- En este último caso, ¿qué tipo de cambios de aplicación requiere para funcionar? ¿Dispone de los recursos para realizar estos cambios?

**La gestión de bots debe ayudar a hacer crecer su negocio, no a frenarlo.**

# 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. Por ejemplo, el scraping de precios de sus páginas de productos, el scraping de su contenido digital de valor añadido o 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?

**Asegúrese de que la solución puede ayudarle a abordar todos sus problemas de bots, independientemente de que afecten a todo el sitio o solo a determinadas páginas.**

# 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 tenga experiencia en su empresa, a veces necesita ayuda adicional: ***necesita expertos que comprendan los problemas de bots.*** 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 de los conocimientos suficientes sobre los recursos específicos en materia de bots para sacar el máximo partido de una solución?
- ¿El proveedor de gestión de bots le ofrece servicios profesionales o solo vende productos?
- ¿Le ofrece asistencia el proveedor para responder a los incidentes de seguridad en cualquier momento, incluso en plena noche?

**Necesita a alguien que pueda establecer una correlación entre sus problemas principales y el tipo de bots, y diseñar e implementar una estrategia capaz de resolverlos.**

# Ni todos los bots son iguales, ni tampoco lo son las soluciones de gestión de bots

Si su sitio web se satura con el tráfico de bots, es posible que, en caliente, caiga en la tentación de comprar cualquier cosa que prometa resolver su problema de bots.

No obstante, antes de comprar impulsivamente, asegúrese de tener en cuenta las 10 principales consideraciones para la gestión de bots a fin de obtener la mejor solución para su situación y necesidades únicas.

Akamai *Intelligent Security Starts at the Edge*

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com o blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en julio de 2020.

Para más información, visita: https://www.dimtec.com
Contactáme: Diana Pardo Pardo, dpardo@dimtec.com

DIMTEC 13
DIGITAL MEDIA TECHNOLOGIES