



Privacidad desde el diseño

Cómo los servicios Akamai Bot Manager Premier y Page Integrity Manager cumplen con los requisitos de privacidad de la UE

Descripción general

Akamai entiende que proteger los datos personales y mantener el cumplimiento de los requisitos de privacidad resulta clave para establecer confianza en nuestra tecnología y nuestros servicios. En este white paper veremos cómo Bot Manager Premier¹ y Page Integrity Manager cumplen con la Directiva sobre privacidad y comunicaciones electrónicas de la UE y con el Reglamento general de protección de datos (RGPD)² para que pueda evaluar los riesgos asociados al uso de estos servicios.

Bot Manager Premier está diseñado para detectar solicitudes de acceso automatizadas en las propiedades web generadas por (ro)bots que simulan el comportamiento humano para recopilar y utilizar los datos de inicio de sesión de los usuarios finales.

Page Integrity Manager detecta el código JavaScript inyectado en esas propiedades con fines abusivos. Una vez que se detectan los bots y los scripts, Akamai los categoriza como actividad maliciosa o no maliciosa en función de sus instrucciones, el conocimiento común y nuestra inteligencia contra amenazas. Las actividades maliciosas se bloquearán, y solo los bots y scripts no maliciosos podrán acceder a sus datos, infraestructura y servidores de origen.

Ambos servicios protegen los datos personales que proporcionan los usuarios finales contra la filtración y el uso indebido. La importancia de la protección contra estas amenazas se demuestra en las recientes infracciones de seguridad y filtraciones de datos experimentadas por [British Airways](#) y [The North Face](#).

Arquitectura de Bot Manager Premier

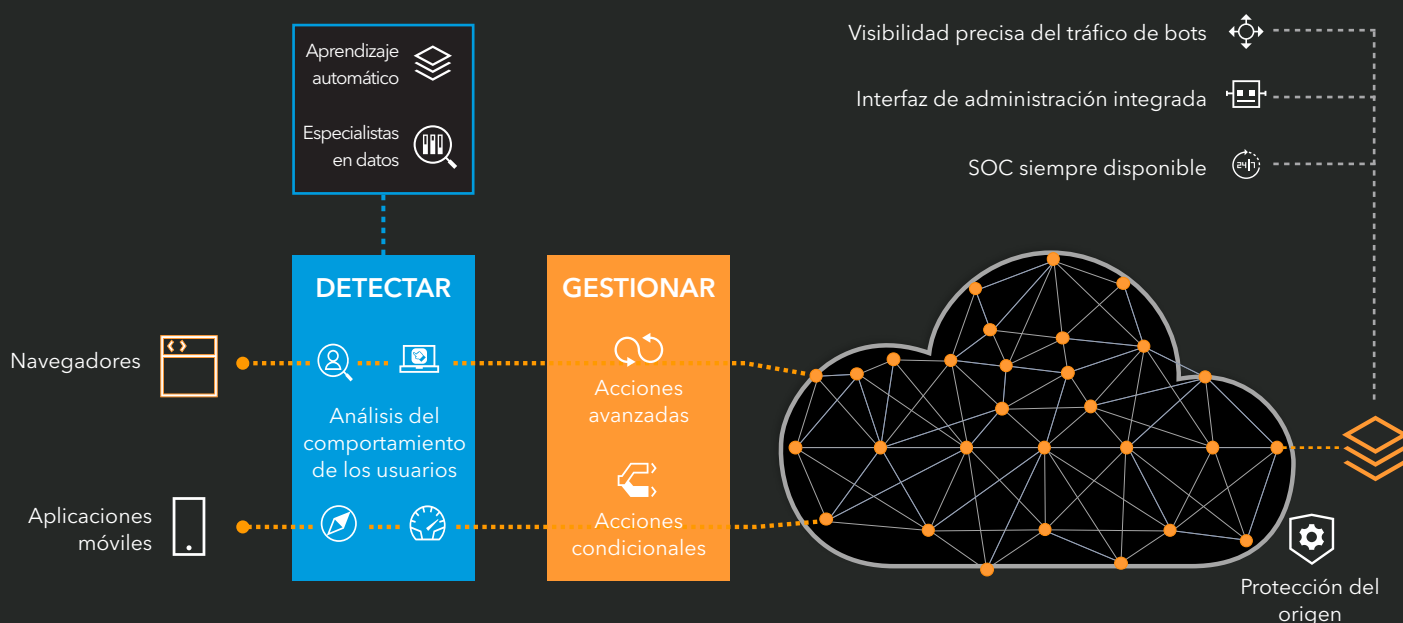


Fig. 1: Arquitectura de Bot Manager Premier

Arquitectura de Page Integrity Manager

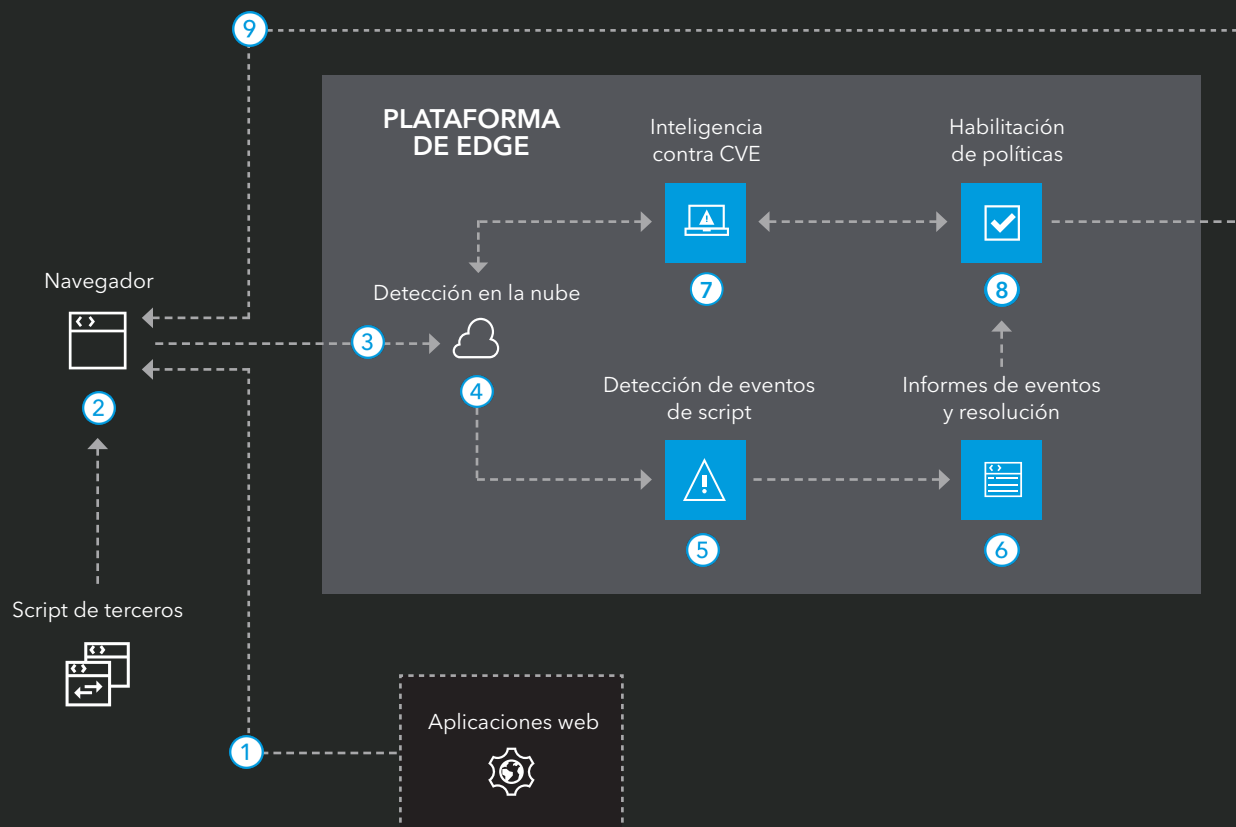


Fig. 2: Arquitectura de Page Integrity Manager

Desde el punto de vista técnico, la detección de bots y scripts se lleva a cabo mediante la inyección de JavaScript o la integración de un kit de desarrollo de software (SDK) para aplicaciones móviles, así como mediante el análisis recopilado de la red, el navegador y los datos de comportamiento. Bot Manager Premier analiza los datos para determinar si la actividad procede de un bot o de un ser humano, mientras que Page Integrity Manager identifica todos los scripts inyectados en las propiedades web. A continuación, cualquier actividad de bots y scripts detectada se clasifica como actividad maliciosa o no maliciosa, y las actividades maliciosas se bloquean para evitar la filtración de datos.

En cuanto a la privacidad, la inyección de JavaScript y la integración del SDK se clasifican como "tecnología de cookies" (según lo estipulado en las leyes de la UE) y activan la aplicación de las leyes sobre privacidad y comunicaciones electrónicas. Además, algunos de los elementos de datos recopilados, como la dirección IP del usuario final, se clasifican como datos personales y activan la aplicación del RGPD.

Cumplimiento de las leyes sobre privacidad y comunicaciones electrónicas de la UE

Para utilizar la tecnología de cookies de Bot Manager Premier y de Page Integrity Manager de conformidad con las leyes de privacidad de la UE, se aplican dos exenciones a las reglas generales: la exención de consentimiento y la exención del mecanismo de exclusión. Estas exenciones permiten colocar Bot Manager Premier y Page Integrity Manager en sus propiedades web para que comiencen a funcionar de inmediato.

Aplicación de la exención de consentimiento

De manera predeterminada, la Directiva sobre privacidad y comunicaciones electrónicas requiere del consentimiento del usuario final para utilizar cualquier tecnología de cookies y recopilar datos relacionados. El único caso en el que no se requiere el consentimiento de un individuo para el uso de cookies y en el que se puede utilizar de inmediato la tecnología de cookies se da cuando la cookie es estrictamente necesaria para proporcionar un servicio de la sociedad de la información (en sus propiedades web) solicitado expresamente por un suscriptor o usuario (el usuario final).³

La mayoría de los miembros de la UE reflejaron esta excepción en sus leyes de transposición de la Directiva sobre privacidad de comunicaciones electrónicas a nivel local.

La tecnología de cookies que se utiliza en Bot Manager Premier y Page Integrity Manager es necesaria para el funcionamiento de los servicios. Sin la inyección de JavaScript, no se pueden recopilar ni analizar datos, y no se detectarán ni bloquearán bots o scripts. La finalidad de la recopilación de datos es proteger los datos personales que se proporcionan a través de sus propiedades web frente a posibles riesgos contra la integridad, filtración y uso indebido. Las autoridades locales de protección de datos confirmaron que el uso de la tecnología de cookies para la prevención de

fraudes y otros servicios de seguridad está dentro de la exención de consentimiento.⁴ La siguiente tabla muestra cómo describe la Oficina del Comisionado de información (ICO, por sus siglas en inglés) del Reino Unido la aplicación de la exención de consentimiento para los servicios de seguridad.⁵

Actividad	¿Es probable que cumpla con una exención?
Seguridad	Según la limitación de la finalidad. Las cookies propias utilizadas con fines de seguridad se pueden basar en la exención estrictamente necesaria; por ejemplo, las cookies que se usan para detectar intentos reiterados de inicio de sesión fallidos. También pueden tener una duración más prolongada que una cookie de sesión. No obstante, las cookies relacionadas con la seguridad de otros servicios online que no sean el suyo sí que requerirán consentimiento. Esto se debe a que la funcionalidad que el usuario ha solicitado está relacionada con su servicio, no con los de terceros. Si utiliza técnicas de huella dactilar de dispositivos con un fin de seguridad específico, también puede confiar en la exención estrictamente necesaria. Sin embargo, al igual que ocurre con las cookies, si la información se procesa con fines secundarios (como los relacionados con la seguridad de servicios online que el usuario no haya solicitado), se necesitará consentimiento. Esto también se aplica cuando la información se procesa con fines de prevención de fraudes, especialmente en casos en los que varios servicios online utilizan un único servicio de prevención de fraudes que procesa la información de los visitantes de todos esos servicios.

Aplicación de la exención de exclusión

Las leyes sobre privacidad y comunicaciones electrónicas exigen a las entidades que ofrezcan a los usuarios finales un mecanismo para rechazar la recopilación de datos mediante tecnología de cookies. Este requisito refleja el derecho a oponerse a ello conforme al artículo 21 del RGPD.⁶

Sin embargo, hay un caso excepcional en el que se abusará de este derecho de control y ejercer una exclusión voluntaria evitará la ejecución de actividades de protección de datos. Este caso particular es el desempeño de un servicio de seguridad basado en la tecnología de cookies.

Rechazar el uso de la tecnología de cookies que se utiliza para detectar bots y scripts maliciosos detiene los servicios de seguridad que protegen contra el acceso no autorizado a datos personales. Siempre que la tecnología de cookies se utilice únicamente con fines de seguridad, la falta de control para el usuario final sobre la recopilación de datos por parte de la tecnología de cookies no vulnera los derechos ni las libertades. Al revés. Esta falta de control garantiza el funcionamiento continuo de la tecnología de cookies que protege los datos personales contra el acceso no autorizado.

Los profesionales de la privacidad de todo el mundo están de acuerdo sobre la necesidad de incorporar esta exención a la exclusión voluntaria: cuando se puede abusar de algún mecanismo de control de datos ofrecido a personas (usuarios finales) para permitir el acceso a los datos sin autorización, el mecanismo de control de datos no tiene sentido y no se debe implementar. En otras palabras, es lógico que el funcionamiento impecable de los servicios de seguridad innovadores prevalezca sobre la necesidad de ofrecer un mecanismo de control de datos (exclusión) relacionado con la tecnología de cookies.⁷

Cumplimiento de la normativa sobre protección de datos de la UE

Bot Manager Premier y Page Integrity Manager procesan los datos de conformidad con el RGPD y otras leyes de privacidad o protección de datos aplicables que incluyen el tipo de datos personales recopilados y la finalidad de la recopilación.

Tipo de datos personales

Bot Manager Premier y Page Integrity Manager recopilan datos de red, del navegador y de comportamiento como, por ejemplo, sesiones TCP, TLS, ID de sesión, agente de usuario, encabezado de solicitud, URL visitadas, fecha y hora, dirección IP del usuario final, configuración del navegador o datos de geolocalización de los servidores de Edge; pero también recopilan datos de comportamiento como toques de pantalla, movimientos del ratón y pulsaciones de teclas.

Finalidad

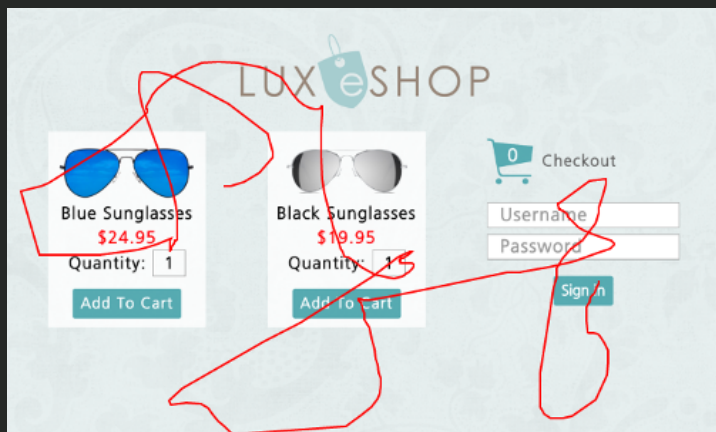
El propósito de recopilar y analizar los datos es detectar bots y scripts maliciosos que simulan el comportamiento humano en sus propiedades web y prevenir que estos filtren datos y se usen de forma indebida.

Para lograr este propósito, Akamai analiza de qué forma se utiliza un dispositivo cuando accede a sus propiedades web. Akamai no identifica al usuario final al realizar este análisis ni crea perfiles de usuarios finales. Además, los datos de comportamiento recopilados no se utilizan con el fin de identificar de manera única a una persona. Por lo tanto, no es necesario clasificar los datos como biométricos según lo estipulado en el RGPD.⁸ Ni tampoco son datos confidenciales (en términos de EE.UU.) ni categorías especiales de datos (en términos de la UE).

Akamai recopila y analiza los datos de comportamiento para determinar si el acceso a su propiedad web lo realiza un bot o un humano, tal como se describe en las siguientes figuras.

Eventos del ratón

Ejemplo humano



Ejemplos de bots

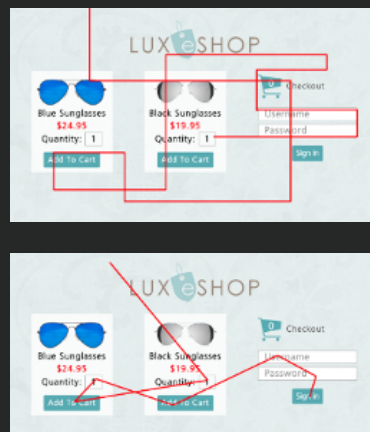
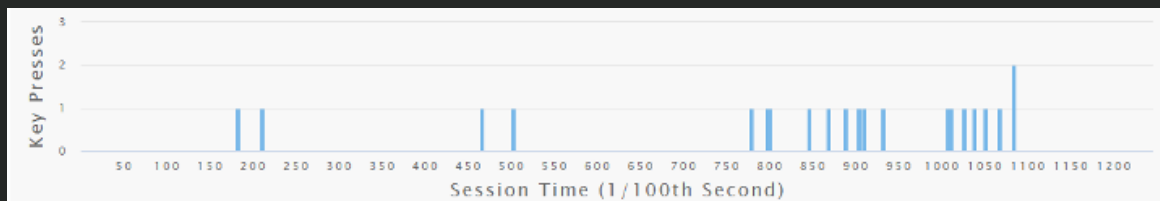


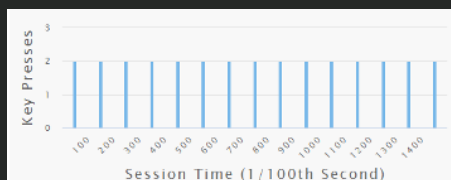
Fig. 3: Los bots sofisticados intentarán ocultarse activando los movimientos del ratón. Se hace así para simular la interacción de un usuario. Sin embargo, después de un determinado número de movimientos, aparecerá un patrón. Akamai puede detectar estos patrones para identificar bots.

Detección de patrones de pulsación de teclas

Pulsaciones de teclas de un humano



Ejemplo de pulsación de teclas de un bot



Ejemplo de pulsación de teclas de un bot

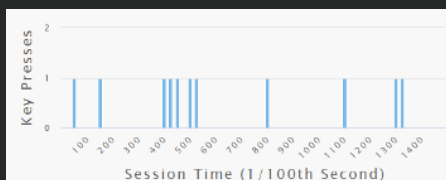


Fig. 4: Por lo general, los seres humanos pulsan teclas de forma más aleatoria incluso que un bot sofisticado. Al examinar la velocidad y la cadencia de las pulsaciones de teclas realizadas por un humano, Akamai puede determinar si un usuario es un bot.

Fundamento jurídico

El fundamento jurídico del procesamiento es el interés legítimo de Akamai por proporcionar servicios de red y de seguridad de la información mediante de detección y bloqueo de bots maliciosos. El interés legítimo es un fundamento jurídico reconocido para el desempeño de servicios de seguridad en virtud del RGPD.⁹

Akamai distribuye y protege hasta un 30 % de todo el tráfico de Internet. Sin sus servicios de administración de bots y scripts, habría muchos más casos de filtración y uso indebido de datos online que vulneraran los derechos y las libertades de los usuarios finales.

Evaluación de la necesidad y la proporcionalidad

El procesamiento de los datos es necesario para que la red de Akamai y los servicios de seguridad de la información se consideren "a la última" con respecto a las leyes de privacidad. Al analizar la red, el navegador y los datos de comportamiento recopilados, Akamai puede determinar con precisión las acciones de bots o humanos y los scripts que se inyectan en una propiedad web.

El análisis de todos los elementos de datos recopilados es proporcionado, teniendo en cuenta la sofisticación de los bots y los scripts actuales. Disminuir la recopilación de datos afecta a la precisión del análisis, lo que se traduce en una detección menos eficaz de las actividades maliciosas. Los bots no se pueden detectar analizando únicamente direcciones IP de usuario final. Si bien los detalles del navegador y de la red indican el uso del dispositivo, se limitan a mecanismos pasivos basados en firmas y son propensos a falsos positivos y falsos negativos. La seguridad innovadora para las propiedades web¹⁰ se extiende a la detección de bots sofisticados. Los bots activos que imitan el comportamiento humano solo se detectan cuando se analizan los datos de comportamiento.

Recopilar más datos sería excesivo, ya que los análisis no mejorarían.

Evaluación de riesgos

El riesgo para los derechos y las libertades de los usuarios finales asociado a las actividades de procesamiento de Bot Manager Premier y de Page Integrity Manager es bajo. Los datos de comportamiento, red y navegador no se clasifican como altamente confidenciales, sensibles ni como una categoría especial de datos personales.¹¹ Las actividades de procesamiento de Akamai relacionadas con Bot Manager Premier y Page Integrity Manager se describen en [la declaración de privacidad de Akamai](#) y se ofrecen de forma transparente a las partes interesadas. Akamai cumple con el principio de minimización de datos, por el cual solo se recopilan los datos necesarios para la detección de bots y JavaScript.

Akamai ha implementado medidas técnicas y organizativas adecuadas para proteger los datos personales procesados contra el acceso no autorizado de terceros. Dichas medidas también se publican de forma transparente en nuestro sitio web: [Programa de seguridad de la información de Akamai](#) y [medidas técnicas y organizativas de Akamai](#).

El análisis para la detección de bots y scripts se realiza en los sistemas Akamai implementados en los Estados Unidos. Por lo tanto, cuando los usuarios finales de la UE acceden a propiedades web protegidas por Bot Manager Premier y Page Integrity Manager, los análisis requieren que se procesen datos personales de la UE en los Estados Unidos. Para garantizar la protección adecuada de los datos mientras se procesan en los Estados Unidos, Akamai ha puesto en práctica las Cláusulas contractuales estándar de la UE dentro del grupo Akamai, con nuestros clientes y subencargados, e implantado protecciones técnicas adicionales para proteger los datos personales durante el procesamiento en Estados Unidos contra el acceso de terceros.

Akamai aplica los mismos requisitos sobre protección de datos en todas las entidades del grupo, independientemente de dónde se encuentren. Hemos implementado medidas complementarias para proteger los datos transferidos contra el acceso de terceros. Además, desde el punto de vista de Akamai, los datos que transfiere Akamai a los Estados Unidos para Bot Manager Premier y Page Integrity Manager no son el tipo de datos que interesan a las agencias de vigilancia de datos (EE. UU.) a la hora de realizar operaciones de vigilancia.¹² La mayoría de los datos son de acceso libre como requisito para establecer una conexión a Internet y un tercero no necesita acudir a Akamai para recopilar estos datos; existen otras muchas formas más prácticas de acceder a esos datos. Por lo tanto, Akamai ha estimado que los riesgos de acceso de terceros a los datos transferidos a los Estados Unidos para Bot Manager Premier y Page Integrity Manager son mínimos. Los detalles se resumen en la [Declaración sobre transferencia de datos de Akamai](#), disponible en el Centro de confianza de privacidad de Akamai.

De conformidad con el principio de minimización y seguridad de los datos, Akamai establece el periodo de retención en 90 días. Este periodo es apropiado si se tiene en cuenta la necesidad de analizar la red, el navegador y los datos de comportamiento durante un determinado periodo en las distintas regiones para lograr una detección de bots y scripts lo más eficaz posible.

Los servicios de detección y administración de bots y scripts de Akamai no solo protegen sus propiedades web, sino que también mejoran el estado general de Internet. Mediante la detección y bloqueo de bots y scripts en Akamai Intelligent Edge Platform, no solo evitamos la filtración y el abuso de los datos personales de usuario final, sino que también obtenemos información sobre amenazas para los servicios de red y seguridad en beneficio de millones de usuarios finales.

Medidas de mitigación

Siempre que Akamai ha identificado riesgos para los derechos y la libertad de los datos sujetos al funcionamiento de los servicios Bot Manager Premier y Page Integrity Manager, los ha mitigado. Cuando se recopilan datos de comportamiento, no se identifica al usuario final. Además, Akamai ha protegido convenientemente los datos personales y ha implementado medidas adicionales para garantizar una protección adecuada de los datos transferidos contra el acceso de terceros.

Resumen

Bot Manager Premier y Page Integrity Manager de Akamai cumplen con las leyes de protección de datos de la UE. La tecnología de cookies que se utiliza para el funcionamiento de los servicios es la estrictamente necesaria y permite la protección de los datos personales del usuario final, por lo que se aplican las excepciones del requisito de consentimiento y del mecanismo de exclusión.

La recopilación de datos necesaria para el funcionamiento de los servicios es legítima, necesaria y equilibrada. Además, las medidas de mitigación que se han tomado garantizan que el riesgo de las actividades de procesamiento para los derechos y las libertades de los usuarios finales sea muy bajo. Las ventajas del uso de Bot Manager Premier y Page Integrity Manager para sus usuarios finales y otros usuarios online superan a los riesgos, ya que todos se benefician de un Internet más seguro.



Akamai Technologies,
Dra. Anna Schmits, jefa de
Privacidad de Datos, EMEA

Fuente:

1. Las afirmaciones hechas en este documento también se aplican al servicio Akamai Bot Manager Standard, excepto en lo relativo al alcance de la recopilación de datos, que se limita a la red y a los datos del navegador. Más información sobre Akamai Bot Manager: https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. Consulte "Privacidad digital", disponible en: <https://ec.europa.eu/digital-single-market/en/online-privacy>
3. Consulte la enmienda al artículo 5 (3) de la Directiva sobre privacidad y comunicaciones electrónicas 2002/58/EC modificada por la Directiva 2006/24/EC, disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.
4. Consulte, por ejemplo, las directrices sobre cookies de la ICO de Reino Unido, disponibles en <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9>, las directrices de la francesa CNIL, disponibles en <https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines>, o las directrices del Comité de protección de datos alemán (únicamente en alemán), disponibles en https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
5. Consulte la guía de cookies de ICP, disponible en: <https://ico.org.uk/for-organizations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16>.
6. Consulte el artículo 21 (1) del RGPD, disponible en: <https://gdpr-info.eu/art-21-gdpr/>.
7. Consulte, por ejemplo, la guía de la ICO, disponible en: <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9>.
8. Consulte el artículo 9 (1) del RGPD, disponible en: <https://gdpr-info.eu/art-9-gdpr/>.
9. Consulte el considerando 49 del RGPD, disponible en: <https://gdpr-info.eu/recitals/no-49/>
10. Tal como se exige en virtud del artículo 32 del RGPD, disponible en: <https://gdpr-info.eu/art-32-gdpr/>
11. Consulte el artículo 9 del RGPD, disponible en: <https://gdpr-info.eu/art-9-gdpr/>
12. Medidas para la salvaguarda de la privacidad en EE.UU. conforme a las cláusulas contractuales estándar y otras bases legales de la UE para la transferencia de datos entre la UE y EE.UU. tras la sentencia Schrems II, septiembre de 2020. Disponible en: <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>



Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. Akamai Intelligent Edge Platform 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 en el borde de Internet, 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, 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 el 21 de marzo.