WHITE PAPER

Privacy by Design

How Akamai Bot Manager Premier and Page Integrity Manager Services Meet EU Privacy Requirements

Overview

Akamai understands that protecting personal data and maintaining compliance with privacy requirements are critical to establishing trust in our technology and services. This white paper outlines how Bot Manager Premier[1] and Page Integrity Manager meet the EU ePrivacy Directive and General Data Protection Regulation (GDPR)[2] so you can assess the risks associated with operating these services.

Bot Manager Premier is designed to detect automated access requests to your web properties generated by (ro)bots that mimic human behavior to collect and exploit end users' login data.

Page Integrity Manager detects JavaScripts injected into those properties for abusive purposes. Once bots and scripts are detected, Akamai categorizes them as nonmalicious and malicious activities in accordance with your instructions, common knowledge, and our threat intelligence. Malicious activities will be blocked, and only nonmalicious bots and scripts will be able to access your origin servers, infrastructure, and data.

Both services secure personal data provided by end users against exfiltration and abuse. The importance of protecting against such threats is demonstrated in the recent security and data breaches experienced by British Airways and The North Face.

Bot Manager Premier Architecture

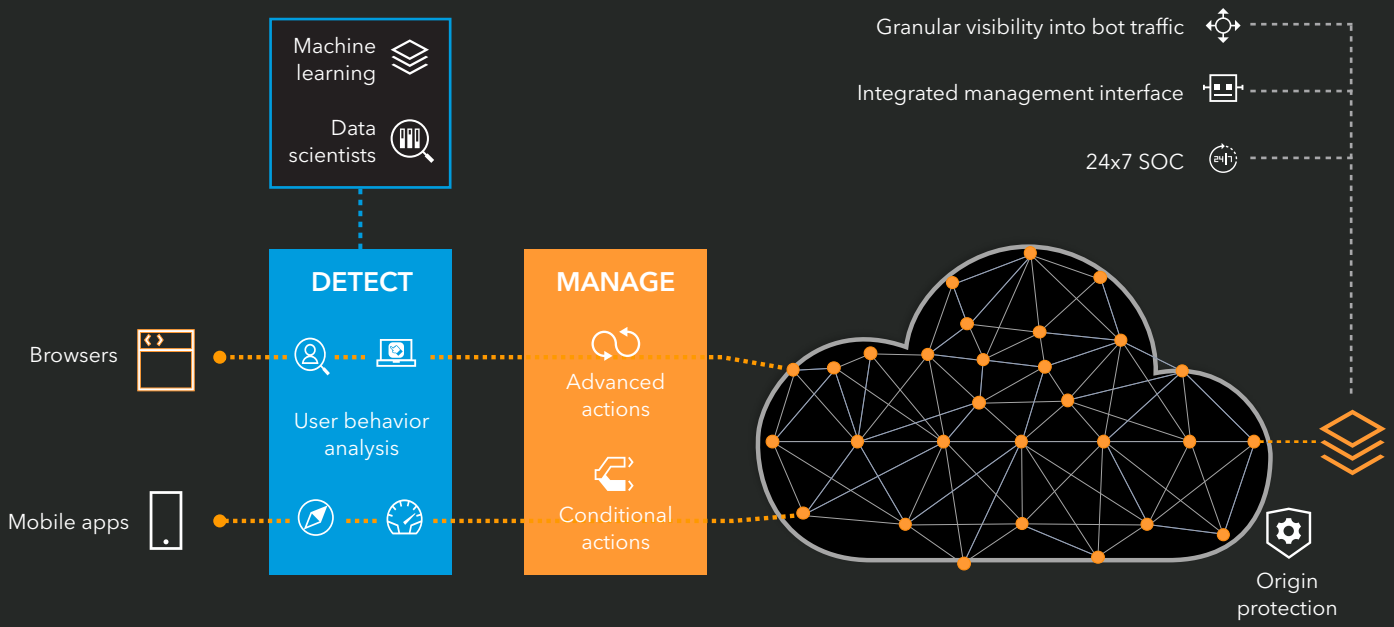


Fig. 1: The Bot Manager Premier architecture

Page Integrity Manager Architecture

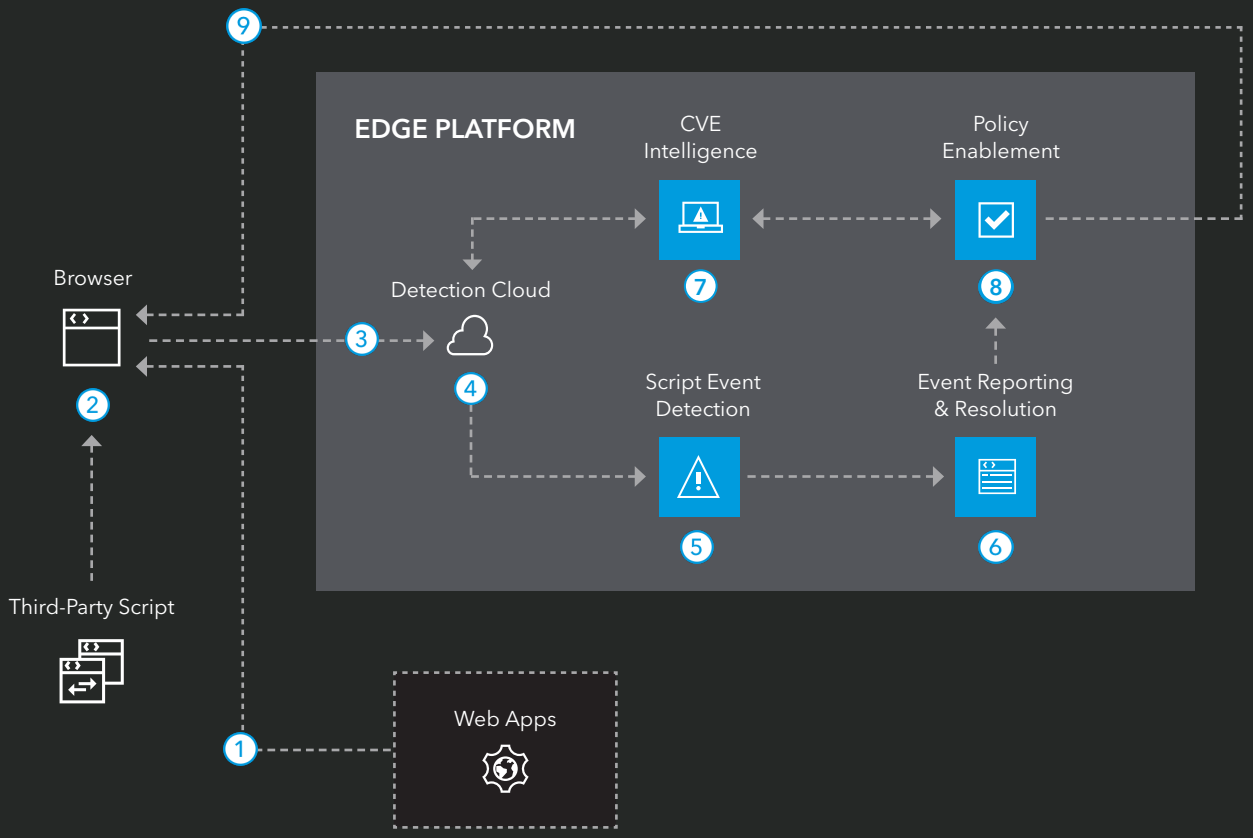


Fig. 2: The Page Integrity Manager architecture

From a technical point of view, bot and script detection is performed via JavaScript injection or mobile app software developer kit (SDK) integration, as well as via the collected analytics of the network, browser, and behavior data. Bot Manager Premier analyzes the data to determine whether the activity originated from a bot or a human, while Page Integrity Manager identifies all the scripts injected into the web properties. Any detected bot and script activities are then categorized as either malicious or nonmalicious activities, and malicious activities are blocked to avoid data exfiltration.

From a privacy perspective, JavaScript injection and SDK integration are classified under EU laws as "cookie technology" and trigger the application of ePrivacy laws. In addition, some of the data elements collected, such as the end user IP address, are classified as personal data and trigger the application of the GDPR.

Compliance with EU ePrivacy laws

To use the Bot Manager Premier and Page Integrity Manager cookie technology in accordance with EU privacy laws, two exemptions from the general rules apply: the consent exemption and opt-out mechanism exemption. These exemptions allow you to place Bot Manager Premier and Page Integrity Manager on your web properties for immediate operation.

Application of the consent exemption

By default, the ePrivacy Directive requires the collection of end-user consent for the usage of any cookie technology and related data collection. Only where the cookie is strictly necessary to provide an information society service (on your web properties) explicitly requested by a subscriber or user (the end user), consent by an individual for the cookie usage is not required and the cookie technology can be operated right away.[3]

Most of the EU members mirrored this exception into their local transposition laws of the ePrivacy Directive.

The cookie technology used for Bot Manager Premier and Page Integrity Manager is necessary for the operation of the services. Without the JavaScript injection, no data can be collected and analyzed, and bots or scripts will not be detected and blocked. The purpose of the data collection is the protection of personal data provided via your web properties against compromise, exfiltration, and abuse. The local data protection authorities confirmed that the usage of cookie technology for fraud prevention and other security services falls within the consent exemption.[4] The following table shows how the UK Information Commissioner's Office (ICO) outlines the application of the consent exemption for security services.[5]

Activity	Likely to meet an exemption?
Security	**Depending on purpose limitation.** First-party cookies used for security purposes can rely on the strictly necessary exemption; for example, cookies used to detect repeated failed login attempts. They can also have a longer duration than a session cookie. However, cookies that relate to the security of other online services besides your own require consent. This is because the functionality the user has requested relates to your service, not those of any others. If you use device fingerprinting techniques for a specific security purpose then you can also rely on the strictly necessary exemption. However, as with cookies, if the information is processed for secondary purposes – such as those relating to the security of online services the user has not requested – consent is required. This also applies where the information is processed for the purposes of fraud prevention, particularly in cases where multiple online services use a single fraud prevention service which processes information from visitors of all of those services.

Application of the opt-out exemption

The ePrivacy laws require entities to offer end users a mechanism to opt out of the data collection by cookie technology. This requirement mirrors the right to object under Article 21 of the GDPR.[6]

However, there is a corner case where this control right will be abused and an opt out exercised will prevent the performance of data protection activities. This corner case is the performance of a security service based on cookie technology.

Opting out of cookie technology used to detect malicious bots and scripts halts security services that protect against unauthorized access to personal data. Provided the cookie technology is solely used for security purposes, the lack of control over the data collection by the cookie technology for the end user does not cause harm to rights and freedoms. In contrast, this lack of control ensures continuous operation of cookie technology that protects personal data against unauthorized access.

Privacy professionals around the world agree on the requirement of this opt-out exemption: Where a data control mechanism offered to individuals (end users) can be abused to enable access to the data in an unauthorized manner, the data control mechanism is meaningless and must not be put in place. In other words, it is common sense that a frictionless operation of state-of-the-art security services prevails over the need to offer a data control (opt-out) mechanism related to cookie technology.[7]

EU data protection compliance

Bot Manager Premier and Page Integrity Manager process data in compliance with the GDPR and other applicable data protection or privacy laws including the type of personal data collected and purpose of collection.

Type of personal data

Bot Manager Premier and Page Integrity Manager collect network, browser, and behavior data like TCP session, TLS session, session ID, user agent, request header, URLs visited, time stamp, end user IP address, browser settings, and geolocation data of edge servers, as well as behavior data like screen touches, mouse movements, and key presses.

Purpose

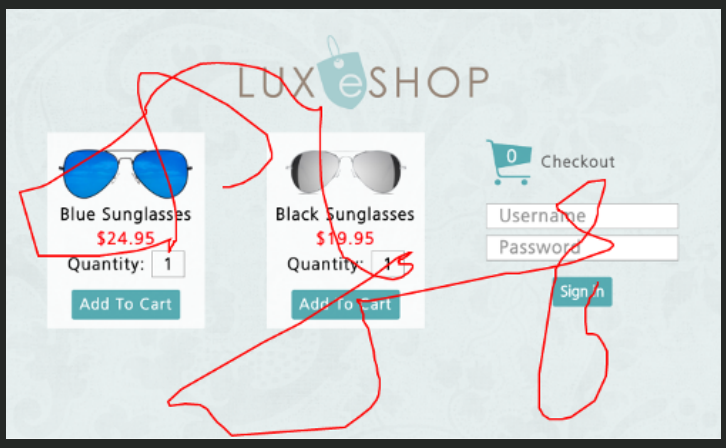
The purpose of collecting and analyzing the data is the detection of malicious bots and scripts mimicking human behavior in your web properties and the prevention of data exfiltration and abuse by them.

To achieve this purpose, Akamai is analyzing the way a device is used when accessing your web properties. Akamai is not identifying the end user when performing this analysis nor creating profiles of end users. In addition, the behavior data collected is not used for the purpose of uniquely identifying an individual. The data therefore does not need to be categorized as biometric data under the GDPR.[8] It is therefore neither sensible data (in US terms) nor special categories of data (in EU terms).

Akamai is collecting and analyzing the behavior data to determine whether the access to your web property is made by a bot or a human as outlined in the figures below.

Mouse Events

Human Example



Bot Examples

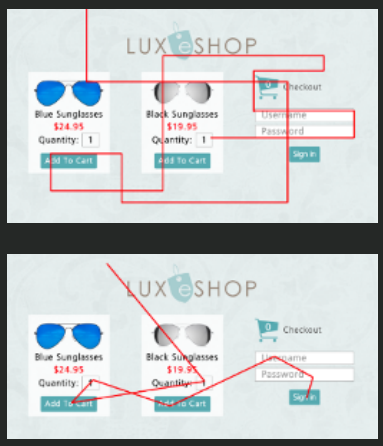
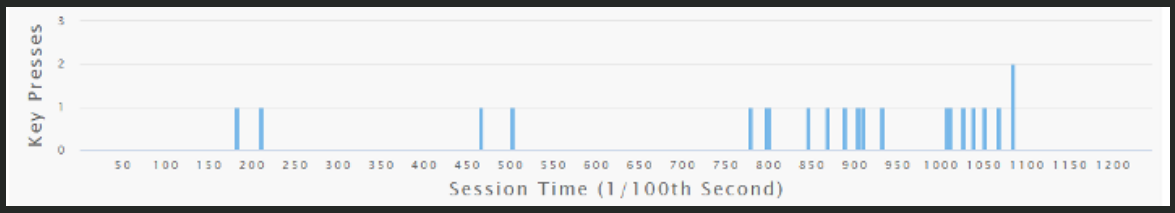


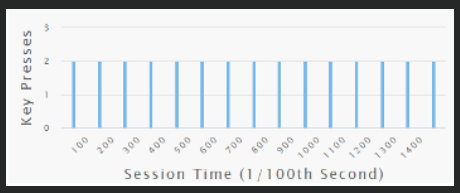
Fig. 3: Sophisticated bots will try to hide by triggering mouse moves. This is designed to emulate a user's interaction. However, after a certain number of moves, a pattern will emerge. Akamai can detect these patterns to identify a bot.

Key Press Pattern Detection

Human Key Presses



Bot Key Press Example



Bot Key Press Example

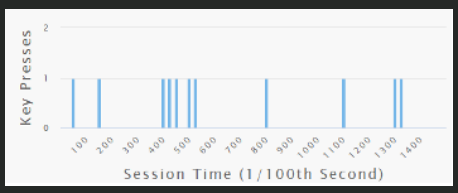


Fig. 4: Humans are usually more random in their key presses than even a sophisticated bot. By examining the velocity and cadence of a human's key presses, Akamai can further determine if a user is a bot.

Legal basis

The legal basis for the processing is Akamai's legitimate interest to provide network and information security services in the form of malicious bot and script detection and blockage. Legitimate interest is a recognized legal basis for the performance of security services under the GDPR.[9]

Akamai delivers and secures up to 30% of all internet traffic. Without its bot and script management services, there would be much more online data exfiltration and data abuse harming the rights and freedoms of end users.

Necessity and proportionality assessment

The processing of the data is necessary for Akamai's network and information security services to be considered state of the art under the privacy laws. By performing analytics of the collected network, browser, and behavior data, Akamai can precisely determine bot or human actions and scripts injected into a web property.

The analytics of all the data elements collected is proportionate considering the sophistication of today's bots and scripts. Reducing data collection impacts the accuracy of the analysis, resulting in less effective detection of malicious activities. Bots cannot be detected by analyzing only end-user IP addresses. While browser and network details indicate device usage, they're limited to passive, signature-based mechanisms and prone to high false positives and false negatives. State-of-the-art security for web properties[10] extends to sophisticated bot detection. Active bots that are mimicking human behavior are detected only where behavior data is analyzed.

Collecting more data would be excessive as the analytics would not improve.

Risk assessment

The risk for the rights and freedoms of the end users associated with the processing activities for Bot Manager Premier and Page Integrity Manager is low. Browser, network, and behavior data is not categorized as highly confidential, sensitive, or a special category of personal data.[11] Akamai's processing activities related to Bot Manager Premier and Page Integrity Manager are described in Akamai's privacy statement, and made transparent to interested parties. Akamai complies with the data minimization principle, collecting only the data necessary for bot and JavaScript detection.

Akamai has appropriate technical and organizational measures in place to secure the processed personal data against unauthorized access by third parties. Such measures are also transparently published on our website: Akamai's Information Security Program and Akamai's Technical and Organizational Measures.

The analytics for bot and script detection are performed on Akamai systems deployed in the United States. Accordingly, where EU end users are accessing web properties protected by Bot Manager Premier and Page Integrity Manager, the analytics require processing of EU personal data in the United States. To ensure adequate data protection when processed in the United States, Akamai has put in place the EU Standard Contractual Clauses within the Akamai group, with our customers and subprocessors, and implemented additional technical safeguards to protect personal data when processed in the United States against third-party access.

Akamai applies the same data protection requirement to all its group entities, independent of the location of the Akamai entity. We have put in place supplemental measures to protect data transferred against third-party access. In addition, in Akamai's view, the data transferred to the United States by Akamai for Bot Manager Premier and Page Integrity Manager is not the type of data (US) surveillance agencies are interested in when performing their surveillance operations.[12] Most of the data is freely accessible as a requirement to establish an internet connection and a third party does not need to approach Akamai to gather such data – many other more convenient ways for third parties to access such data exist. Accordingly, Akamai assessed the risks of third-party access to the data transferred to the United States for Bot Manager Premier and Page Integrity Manager to be minimal. Details are outlined in Akamai's Data Transfer Statement in the Akamai Privacy Trust Center.

Complying with the data minimization and data security principle, Akamai set the retention period to 90 days. This period is appropriate considering the need to analyze the network, browser, and behavior data over a certain period across regions to enable the most effective bot and script detection.

The bot and script detection and management services Akamai provides not only secure your web properties, but also improve the state of the internet overall. By detecting and blocking bots and scripts on the Akamai Intelligent Edge Platform, we not only prevent the exfiltration and abuse of your end-user personal data, but also gain threat intelligence for network and security services to the benefit of millions of end users.

Mitigation measures

Where Akamai identified a risk for the rights and freedom of the data subject by the operation of Bot Manager Premier and Page Integrity Manager services, it mitigated these risks. When collecting behavior data, the end user is not identified. In addition, Akamai has appropriately secured the personal data and put in place supplemental measures to ensure that transferred data is adequately secured against third-party access.

Summary

Akamai Bot Manager Premier and Page Integrity Manager comply with EU data protection laws. The cookie technology used for the operation of the services are strictly necessary and enable the protection of end user's personal data, so the consent requirement and the opt-out mechanism exemptions apply.

The data collection required to operate the services is legitimate, necessary, and proportionate. Furthermore, the mitigation measures taken ensure that the risk of the processing activities for the rights and freedoms of the end users is very low. The benefits from the performance of Bot Manager Premier and Page Integrity Manager to your end users and others online outweigh the risks, as everyone benefits from a more secure internet.

Akamai Technologies
Dr. Anna Schmits, EMEA DPO

Sources:

1. The statements made herein, also apply to Akamai Service Bot Manager Standard, except for the scope of data collection, which is limited to network and browser data. Learn more about Akamai Bot Manager: https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. See "Digital privacy," available at: https://ec.europa.eu/digital-single-market/en/online-privacy
3. See amendment of Article 5 (3) of the ePrivacy Directive 2002/58/EC by Directive 2006/24/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.
4. See, for example, the cookie guidelines by the UK's ICO, available at 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, the guidelines by the French CNIL, available at https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines, or the guidelines by the Committee of the German Authorities (German only), available at https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
5. See the ICP's cookie guidance, available at: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16.
6. See Article 21 (1) GDPR, available at: https://gdpr-info.eu/art-21-gdpr/.
7. See, for example, the ICO's guidance, available at: 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. See Article 9 (1) GDPR, available at: https://gdpr-info.eu/art-9-gdpr/.
9. See Recital 49 GDPR, available at: https://gdpr-info.eu/recitals/no-49/
10. As required under Article 32 GDPR, available at: https://gdpr-info.eu/art-32-gdpr/
11. See Article 9 GDPR, available at: https://gdpr-info.eu/art-9-gdpr/
12. U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, Sept. 2020. Available at: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit **www.akamai.com**, **blogs.akamai.com**, or **@Akamai** on Twitter. You can find our global contact information at **www.akamai.com/locations**. Published 03/21.