개인정보 보호를 고려한 설계

Akamai의 Bot Manager Premier 및 Page Integrity Manager가 EU 개인정보 보호 요구사항을 준수하는 방법

Overview

Akamai는 개인정보를 보호하고 개인정보 보호 요구사항을 준수하는 것이 Akamai의 기술과 서비스에 대한 신뢰 구축에 반드시 필요하다는 사실을 알고 있습니다. 이 백서는 Bot Manager Premier[1] 및 Page Integrity Manager가 EU ePrivacy Directive 및 GDPR(General Data Protection Regulation)[2] 을 준수하는 방법을 설명합니다. 따라서 이런 솔루션을 사용할 때 직면하게 되는 리스크를 평가할 수 있습니다.

Bot Manager Premier는 사람의 행동을 모방해 사용자의 로그인 데이터를 수집·악용하는 로봇/봇이 웹 자산에 보내는 자동화된 접속 요청을 탐지하도록 설계되었습니다. Page Integrity Manager는 악의적인 목적으로 이러한 자산에 삽입된 자바스크립트를 탐지합니다. Akamai는 봇과 스크립트를 탐지하면 고객의 지침, 일반 지식, Akamai의 위협 인텔리전스를 기반으로 봇을 정상 활동과 악성 활동으로 분류합니다. 악성 활동은 차단되고 정상 봇과 스크립트만 오리진 서버와 인프라 및 데이터에 접속할 수 있습니다.

두 서비스 모두 사용자의 개인정보가 유출되거나 악용되지 않도록 보호합니다. 최근 British Airways와 North Face에 발생한 보안 사고 및 데이터 유출은 이러한 위협을 방어하는 것이 얼마나 중요한지 알려줍니다.

Bot Manager Premier 아키텍처

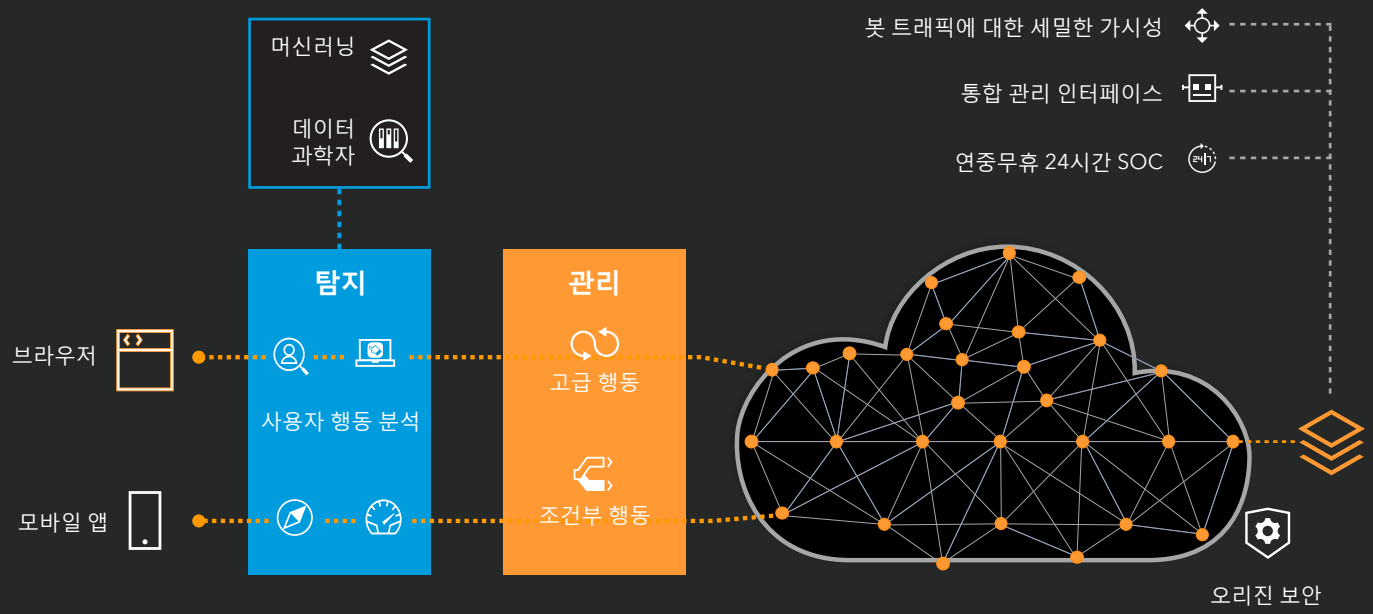


그림 1: Bot Manager Premier 아키텍처

Page Integrity Manager 아키텍처

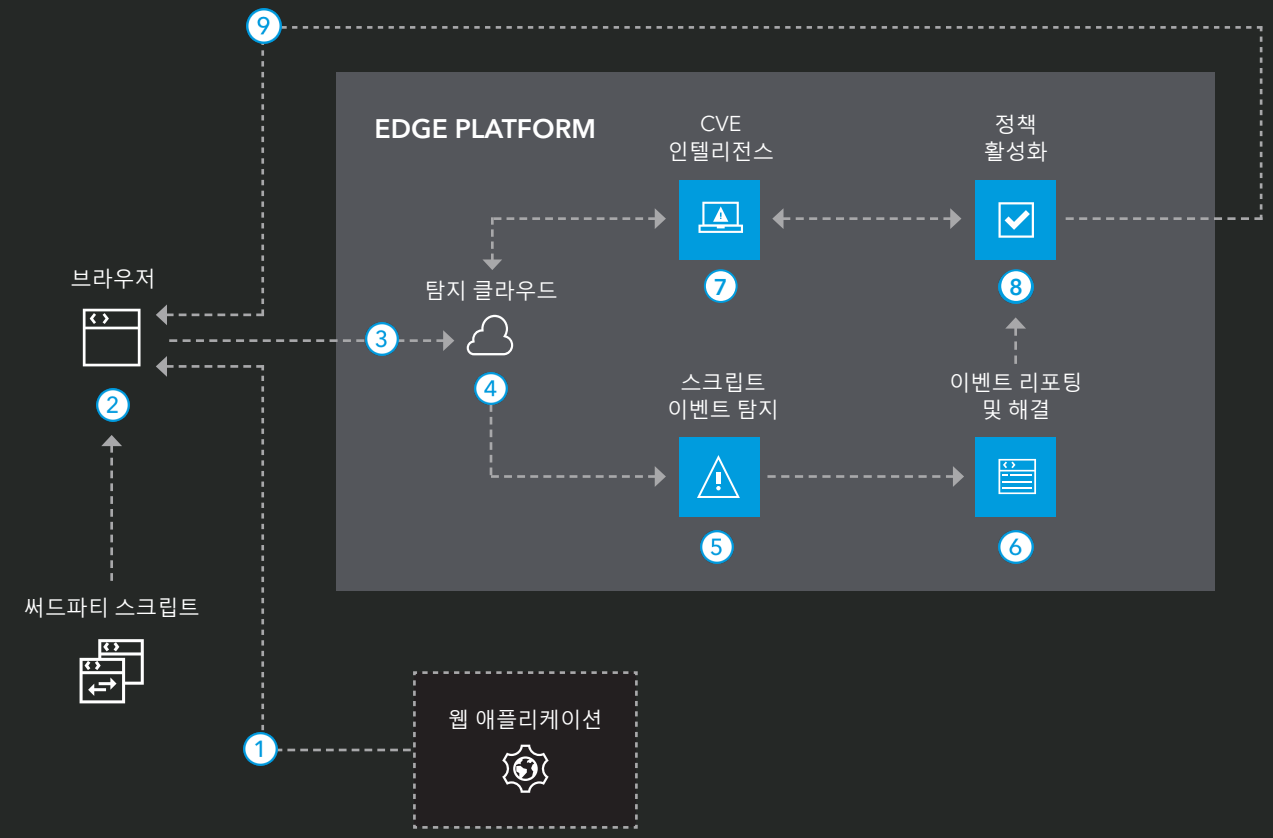


그림 2: Page Integrity Manager 아키텍처

기술적으로 봇과 스크립트를 탐지하려면 수집된 네트워크, 브라우저, 행동 데이터를 분석하고 자바스크립트 삽입 또는 모바일 앱 SDK(Software Developer Kit) 통합이 이루어져야 합니다. Bot Manager Premier는 데이터를 분석하여 해당 활동의 주체가 봇인지, 사람인지 확인합니다. Page Integrity Manager는 웹 자산에 삽입된 모든 스크립트를 식별합니다. 탐지된 봇 활동과 스크립트 활동은 악성 또는 정상으로 분류되며, 악성 활동은 데이터 유출을 방지하기 위해 차단됩니다.

개인정보 보호 측면에서 자바스크립트 삽입 및 SDK 통합은 EU 법률에 따라 '쿠키 기술'로 분류되며 ePrivacy 법의 적용을 받습니다. 또한 사용자 IP 주소 등 수집된 데이터 요소 중 일부는 개인정보로 분류되어 GDPR의 적용을 받습니다.

EU ePrivacy 법 준수

EU 개인정보 보호법에 따라 Bot Manager Premier 및 Page Integrity Manager 쿠키 기술을 사용하면 일반적인 원칙에서 2가지 예외 조건(동의 면제 및 옵트아웃 메커니즘 면제)이 적용됩니다. 이러한 예외 조건에 따라 Bot Manager Premier 및 Page Integrity Manager를 웹 자산에 적용해 즉각적으로 운영할 수 있습니다.

동의 면제 신청

기본적으로 ePrivacy Directive는 쿠키 기술 및 관련 데이터 수집 사용에 대한 사용자 동의를 수집할 것을 요구합니다. 구독자 또는 사용자(최종 사용자)가 명시적으로 요청한 정보 사회 서비스(사용자의 웹 속성에 포함)를 제공하기 위해 쿠키가 반드시 필요한 경우에만 쿠키 사용에 대한 개인의 동의가 필요하지 않으며 쿠키 기술을 즉시 사용할 수 있습니다.[3]

대부분의 EU 회원국은 이 예외 조건을 ePrivacy Directive의 현지 전환법에 반영했습니다.

Bot Manager Premier 및 Page Integrity Manager에 사용되는 쿠키 기술은 서비스 운영에 필수적입니다. 자바스크립트 삽입이 없으면 데이터를 수집·분석할 수 없으며, 봇이나 스크립트를 탐지하거나 차단할 수 없습니다. 데이터 수집의 목적은 웹 자산을 통해 제공되는 개인정보가 손상·유출·악용되지 않게 보호하는 것입니다. 현지 데이터 보호 당국은 쿠키 기술을 사기 방지 및 기타 보안 서비스에 사용하는 것이 동의 면제 범위에 포함된다고 확인했습니다.[4] 다음 표에는 영국 정보위원회(ICO)가 보안 서비스에 대한 동의 면제를 적용한다고 명시한 내용이 나타나 있습니다.[5]

활동	예외 조건에 부합합니까?
보안	**목적 제한에 따라 다릅니다.** 보안을 위해 사용되는 퍼스트파티 쿠키는 반드시 필요한 예외조건(예: 반복된 로그인 시도 실패를 탐지하는 데 사용되는 쿠키)에 의존할 수 있습니다. 기간이 세션 쿠키보다 더 길 수도 있습니다. 그러나 사용자 본인 외 다른 온라인 서비스의 보안과 관련된 쿠키는 동의가 필요합니다. 이는 사용자가 요청한 기능이 다른 사람이 아닌 사용자의 서비스와 관련이 있기 때문입니다. 디바이스 지문 인식 기술을 특정 보안 목적으로 사용하는 경우 반드시 필요한 예외 조항을 적용할 수도 있습니다. 그러나 쿠키와 마찬가지로 부차적인 목적(사용자가 요청하지 않은 온라인 서비스의 보안 관련 등)으로 정보를 처리하는 경우에는 동의가 필요합니다. 또한 사기를 방지하기 위해 정보를 처리하는 경우, 특히 여러 온라인 서비스에서 단일 사기 방지 서비스를 통해 모든 서비스 방문자의 정보를 처리하는 경우에도 마찬가지입니다.

옵트아웃 예외의 적용

ePrivacy 법에 의하면 기업은 쿠키 기술에 의한 데이터 수집을 옵트아웃할 수 있는 메커니즘을 사용자에게 제공해야 합니다. 이 요구사항은 GDPR 제21조에 의거한 거부권을 반영합니다.[6]

그러나 예외적으로 이 제어 권한이 남용되고 옵트아웃으로 인해 데이터 보호 활동의 효과가 저하되는 사례가 있습니다. 이 예외 사례는 쿠키 기술을 기반으로 한 보안 서비스의 실행입니다.

악성 봇과 악성 스크립트를 탐지하는 데 사용되는 쿠키 기술을 옵트아웃하면 개인정보에 대한 무단 접속을 방지하는 보안 서비스가 중단됩니다. 쿠키 기술을 보안 목적으로만 사용할 때는 사용자를 위한 쿠키 기술이 수집한 데이터에 대한 제어가 부족하다 해도 권리와 자유가 침해되지 않습니다. 반대로 이러한 제어가 없으면 개인정보를 무단 접속으로부터 보호하는 쿠키 기술이 계속 작동합니다.

전 세계의 개인정보 보호 전문가들은 이 옵트아웃 예외 요건에 동의합니다. 개인(사용자)에게 제공되는 데이터 제어 메커니즘이 데이터에 대한 무단 접속으로 악용될 수 있다면 데이터 제어 메커니즘은 의미가 없으며 절대로 사용하지 말아야 합니다. 다시 말해, 쿠키 기술과 관련된 데이터 제어(옵트아웃) 메커니즘을 제공하는 것보다 첨단 보안 서비스를 원활하게 운영하는 것이 당연히 더 중요합니다.[7]

EU 데이터 보호 컴플라이언스

Bot Manager Premier 및 Page Integrity Manager는 데이터를 처리할 때 GDPR 및 기타 관련 데이터 보호법, 개인정보 보호법을 준수하고 수집된 개인정보의 종류 및 수집 목적을 고려합니다.

개인정보의 종류

Bot Manager Premier 및 Page Integrity Manager는 네트워크와 브라우저 및 TCP 세션과 TLS 세션, 세션 ID, 사용자 에이전트, 요청 헤더, 방문한 URL, 타임 스탬프, 사용자 IP 주소, 브라우저 설정, 엣지 서버의 지리적 위치 데이터와 같은 행동 데이터와 스크린 터치, 마우스 이동, 키 누름과 같은 행동 데이터를 수집합니다.

목적

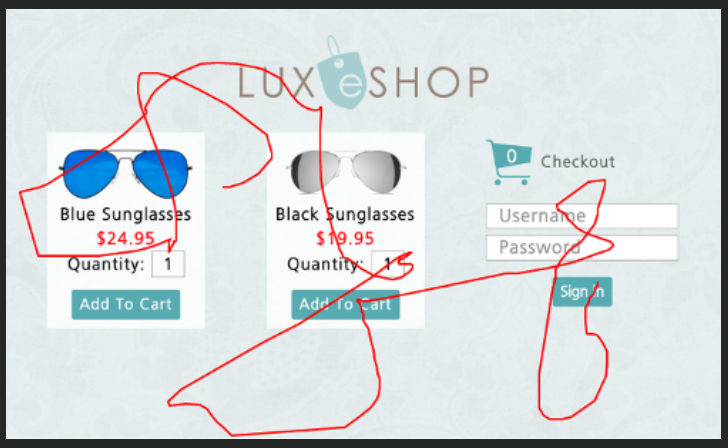
데이터를 수집·분석하는 목적은 웹 자산에서 사용자 행동을 모방하는 악성 봇과 악성 스크립트를 탐지하고, 봇의 데이터 유출·악용을 방지하는 것입니다.

이러한 목적을 달성하기 위해 Akamai는 웹 자산에 접속할 때 디바이스가 사용되는 방식을 분석하고 있습니다. Akamai는 이 분석을 수행하거나 사용자의 프로필을 생성할 때 사용자를 식별하지 않습니다. 또한 특정 개인을 고유하게 식별하기 위해 추가 정보를 수집하지 않습니다. 따라서 이 데이터는 GDPR에 따라 생체 인식 데이터로 분류되지 않아도 됩니다.[8] 이 데이터는 감각 데이터(미국 용어)도 아니고 데이터의 특수 범주(EU 용어)에 속하지도 않습니다.

Akamai는 아래 그림에 나타난 바와 같이 사용자 웹 자산에 접속하려는 주체가 봇인지 사람인지 판단하기 위해 행동 데이터를 수집·분석합니다.

마우스 이벤트

인간 행동 예시



봇 행동 예시

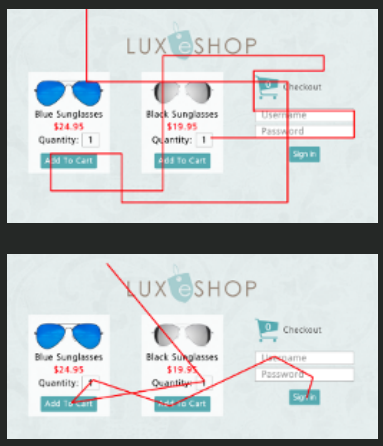
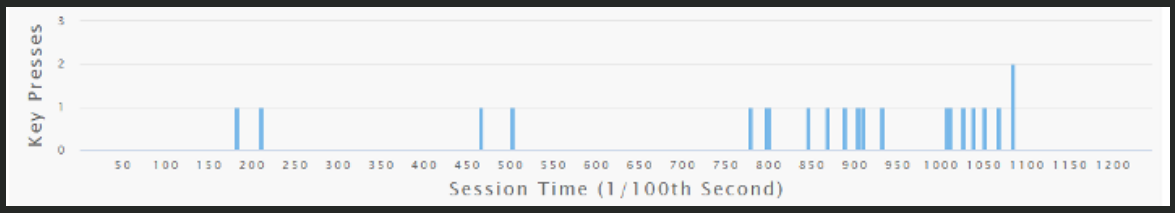


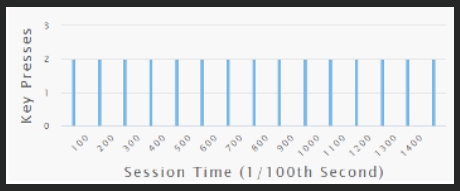
그림 3: 정교한 봇은 마우스 움직임을 트리거하여 은폐를 시도할 것입니다. 이것은 사용자의 상호작용을 모방하기 위해서입니다. 하지만 일정 횟수 이상으로 움직인 후에는 패턴이 나타납니다. Akamai는 이러한 패턴을 탐지하여 봇을 식별할 수 있습니다.

키 누름 패턴 탐지

인간 키 누름



봇 키 누름 예시



봇 키 누름 예시

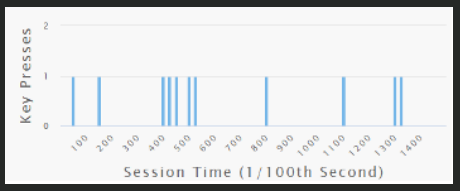


그림 4: 일반적으로 인간의 키 누름은 정교한 봇보다 더 불규칙합니다. Akamai는 사람이 키를 누를 때의 속도와 리듬을 조사해 사용자가 봇인지 여부를 더욱 구체적으로 파악할 수 있습니다.

법적 근거

이 처리에 대한 법적 근거는 악성 봇과 악성 스크립트 탐지 및 차단의 형태로 네트워크 및 정보 보안 서비스를 제공하는 Akamai의 정상적인 권리입니다. GDPR에 따라 보안 서비스를 수행할 수 있는 인정된 법적 근거입니다.[9]

Akamai는 전체 인터넷 트래픽의 최대 30%를 처리·보호합니다. 봇 및 스크립트 관리 서비스가 없다면 사용자의 권리와 자유를 해치는 온라인 데이터 유출 및 데이터 악용이 크게 증가할 것입니다.

필요성 및 비례 평가

데이터 처리는 Akamai의 네트워크 및 정보 보안 서비스가 개인정보 보호법에 따라 최첨단 기술로 간주되기 위해 반드시 필요합니다. Akamai는 수집된 네트워크 데이터와 브라우저 데이터 및 행동 데이터를 분석함으로써 행동의 주체가 봇인지 사람인지 여부와 웹 자산에 삽입된 스크립트를 정확하게 파악할 수 있습니다.

오늘날의 봇과 스크립트의 정교함을 고려할 때 수집된 모든 데이터 요소의 분석은 비례적입니다. 수집된 데이터가 감소하면 분석의 정확도에 영향을 끼쳐 악성 활동을 효과적으로 탐지하지 못하게 됩니다. 사용자 IP 주소 분석만으로는 봇을 탐지할 수 없습니다. 브라우저 및 네트워크 세부 정보를 통해 디바이스 사용을 알 수 있지만 수동적인 시그니처 기반의 메커니즘으로 제한되며 오탐률과 미탐률이 높습니다. 최첨단 웹 자산 보안 기술[10]은 정교한 봇도 탐지할 수 있습니다. 사람의 행동을 모방하는 봇은 행동 데이터를 분석하는 곳에서만 탐지 가능합니다.

분석이 개선되지 않으면 추가 데이터 수집은 의미가 없습니다.

리스크 평가

Bot Manager Premier 및 Page Integrity Manager의 처리 활동으로 사용자의 권리와 자유가 침해당할 리스크는 낮습니다. 브라우저, 네트워크, 행동 데이터는 상당한 기밀이나 주요 범주 또는 특수 범주의 개인정보로 분류되지 않습니다.[11] Bot Manager Premier 및 Page Integrity Manager와 관련된 Akamai의 처리 활동은 Akamai의 개인정보 취급방침에 설명되어 있으며, 이해당사자들에게 투명하게 공개되어 있습니다. Akamai는 봇 탐지 및 자바스크립트 탐지에 필요한 데이터만 수집하여 데이터 최소화 원칙을 준수합니다.

Akamai는 처리된 개인정보에 제3자가 무단으로 접속하지 못하도록 보호하기 위한 적절한 기술적·조직적 조치를 하고 있습니다. 이러한 조치는 Akamai의 정보 보안 프로그램과 Akamai의 기술적·조직적 조치에 투명하게 게시됩니다.

봇 탐지 및 스크립트 탐지는 미국에 배치된 Akamai 시스템이 분석합니다. 따라서 EU 사용자가 Bot Manager Premier 및 Page Integrity Manager의 보호를 받는 웹 자산에 접속할 때 미국에서 개인정보를 처리해야 분석할 수 있습니다. Akamai는 미국에서 처리하는 데이터를 적절히 보호하기 위해 Akamai 그룹과 고객사 및 보조 처리사 간에 EU 표준 계약 조항을 마련했고, 미국에서 처리하는 개인정보에 써드파티가 접속하지 못하도록 하기 위해 기술적 보안 조치를 추가적으로 실행했습니다.

Akamai는 Akamai 법인의 위치와 관계없이 모든 그룹 법인에 동일한 데이터 보호 요구사항을 적용합니다. 전송되는 데이터를 써드파티 접속으로부터 보호하기 위한 추가 조치를 마련했습니다. 또한 Akamai의 관점에서 볼 때 Akamai가 Bot Manager Premier 및 Page Integrity Manager 처리를 위해 미국으로 전송하는 데이터는 데이터 감시 기관이 관심을 기울이는 데이터 종류(미국)가 아닙니다.[12] 대부분의 데이터는 인터넷을 연결하기 위한 요구사항이므로 자유롭게 접속할 수 있으며, 써드파티는 데이터를 수집하기 위해 Akamai에 접근할 필요가 없습니다. 해당 데이터에 접속할 수 있는 다른 여러 가지 편리한 방법이 있기 때문입니다. 따라서 Akamai는 Bot Manager Premier 및 Page Integrity Manager 처리를 위해 미국으로 전송하는 데이터에 대한 써드파티 접속의 리스크를 최소화했습니다. 자세한 내용은 Akamai 프라이버시 트러스트 센터의 Akamai의 데이터 전송 설명문에서 확인하실 수 있습니다.

Akamai는 데이터 최소화 및 데이터 보안 원칙에 따라 보존 기간을 90일로 설정합니다. 가장 효과적으로 봇 및 스크립트를 탐지하기 위해 특정 기간 모든 지역에 걸쳐 네트워크, 브라우저, 행동 데이터를 분석해야 한다는 점을 고려하면 적절한 기간입니다.

Akamai가 제공하는 봇 탐지 및 스크립트 탐지 및 관리 서비스는 웹 자산을 안전하게 보호할 뿐 아니라 전반적인 인터넷 상태를 개선합니다. Akamai Intelligent Edge Platform에서 봇 및 스크립트를 탐지·차단함으로써 사용자의 개인정보가 유출되고 악용되는 것을 막을 뿐 아니라 네트워크 및 보안 서비스에 대한 위협 인텔리전스를 확보하여 수백만 사용자에게 혜택을 제공합니다.

방어 조치

Akamai는 Bot Manager Premier 서비스 및 Page Integrity Manager 서비스를 운영하여 데이터 주체의 권리와 자유를 침해하는 리스크를 파악하고 해당 리스크를 완화했습니다. 행동 데이터를 수집할 때 사용자는 식별하지 않습니다. 또한 Akamai는 개인정보를 적절히 보호하고, 전송된 데이터를 써드파티 접속으로부터 적절히 보호하는 보완 조치를 마련했습니다.

요약

Akamai Bot Manager Premier 및 Page Integrity Manager는 EU 데이터 보호법을 준수합니다. 서비스 운영 시 사용하는 쿠키 기술은 반드시 필요하며 사용자의 개인정보를 보호하기 때문에 동의 요구사항 및 옵트아웃 메커니즘 예외가 적용됩니다.

서비스 운영에 필요한 데이터 수집은 정상적이고 필요하며 적절합니다. 또한 완화 조치를 마련했기 때문에 처리 활동으로 인한 사용자의 권리와 자유가 침해될 리스크는 매우 낮습니다. 모든 사람들에게 보다 안전한 인터넷을 제공하기 때문에 Bot Manager Premier 및 Page Integrity Manager를 통해 얻는 장점은 리스크보다 훨씬 큽니다.

Akamai Technologies
EMEA DPO 안나 슈미츠
(Anna Schmits) 박사

출처:

1. 본 내용은 네트워크 및 브라우저 데이터로 제한되는 데이터 수집 범위를 제외한 Akamai Service Bot Manager Standard에도 적용됩니다. Akamai Bot Manager에 대해 자세히 알아보시기 바랍니다. https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. 다음 웹사이트에서 '디지털 개인정보 보호'를 참조하세요. https://ec.europa.eu/digital-single-market/en/online-privacy
3. 다음 웹사이트에서 'Directive 2002/58/EC 제5조 제3항의 개정에 관한 Directive 2006/24/EC'를 참조하세요. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.
4. 예를 들어, 영국 ICO의 쿠키 지침은 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/#rules9에서, 프랑스 CNIL의 지침은 https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines에서, 독일 당국의 위원회가 발행한 지침(독어로만 제공)은 https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf에서 참조하세요.
5. ICP의 쿠키 지침은 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/#comply16에서 참조하세요.
6. 다음 웹사이트에서 GDPR의 제21조 제1항을 참조하세요. https://gdpr-info.eu/art-21-gdpr/.
7. 예를 들어 ICO의 지침은 다음 웹사이트에서 참조하세요. 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. 다음 웹사이트에서 GDPR의 제9조 제1항을 참조하세요. https://gdpr-info.eu/art-9-gdpr/.
9. 다음 웹사이트에서 GDPR 설명조항 49를 참조하세요. https://gdpr-info.eu/recitals/no-49/
10. GDPR 제32조에 따라 다음 웹사이트에서 참조하세요. https://gdpr-info.eu/art-32-gdpr/
11. 다음 웹사이트에서 GDPR 제9조를 참조하세요. https://gdpr-info.eu/art-9-gdpr/
12. 2020년 9월의 Schrems II 판결 이후 유럽 및 미국 간 데이터 전송에 대한 SCC 및 기타 법적 근거 관련한 미국 개인정보 보호 조치. 다음 웹사이트에서 참조하세요. https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 인텔리전트 엣지 플랫폼은 기업과 클라우드 등 모든 곳으로 확장하고 있으며, 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2021년 03월 발행.