WHITE PAPER

Privacidade por meio de design

Como os serviços Bot Manager Premier e Page Integrity Manager da Akamai atendem aos requisitos de privacidade da UE

Visão geral

A Akamai entende que proteger os dados pessoais e manter a conformidade com os requisitos de privacidade é essencial para estabelecer a confiança em nossa tecnologia e nossos serviços. Este white paper descreve como o Bot Manager Premier[1] e o Page Integrity Manager atendem à Diretiva de privacidade eletrônica da UE e ao GDPR (General Data Protection Regulation, Regulamento geral de proteção de dados)[2] para que você possa avaliar os riscos associados à operação desses serviços.

O Bot Manager Premier foi projetado para detectar solicitações automatizadas de acesso às suas propriedades na Web geradas por (ro)bots que imitam o comportamento humano a fim de coletar e explorar os dados de login dos usuários finais. O Page Integrity Manager detecta JavaScripts mal-intencionados injetados nessas propriedades com objetivos de violação. Depois que os bots e scripts são detectados, a Akamai os classifica como atividades não maliciosas e mal-intencionadas de acordo com suas instruções, conhecimento comum e nossa inteligência contra ameaças. As atividades mal-intencionadas serão bloqueadas, e somente bots e scripts não maliciosos poderão acessar seus servidores de origem, infraestrutura e dados.

Os dois serviços protegem os dados pessoais fornecidos pelos usuários finais contra exfiltração e violação. A importância da proteção contra essas ameaças é demonstrada nas recentes violações de segurança e dados enfrentadas pela British Airways e pela The North Face.

Arquitetura do Bot Manager Premier

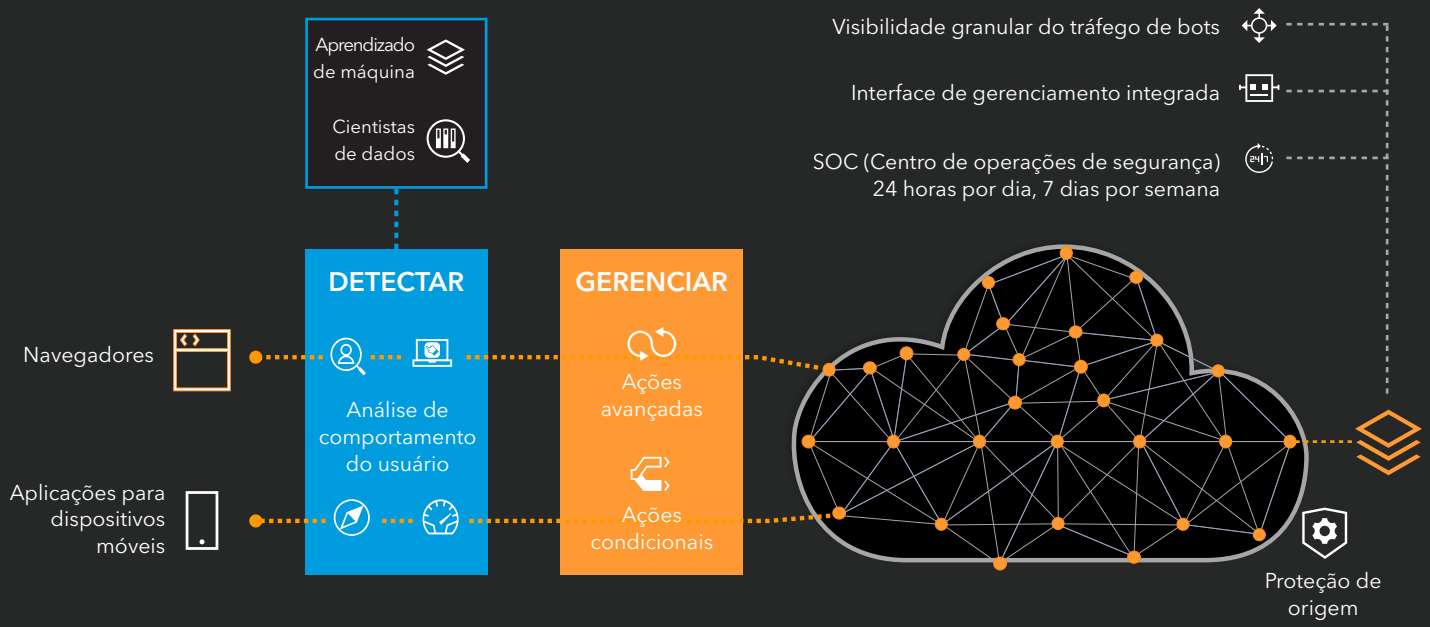


Fig. 1: A arquitetura do Bot Manager Premier

Arquitetura do Page Integrity Manager

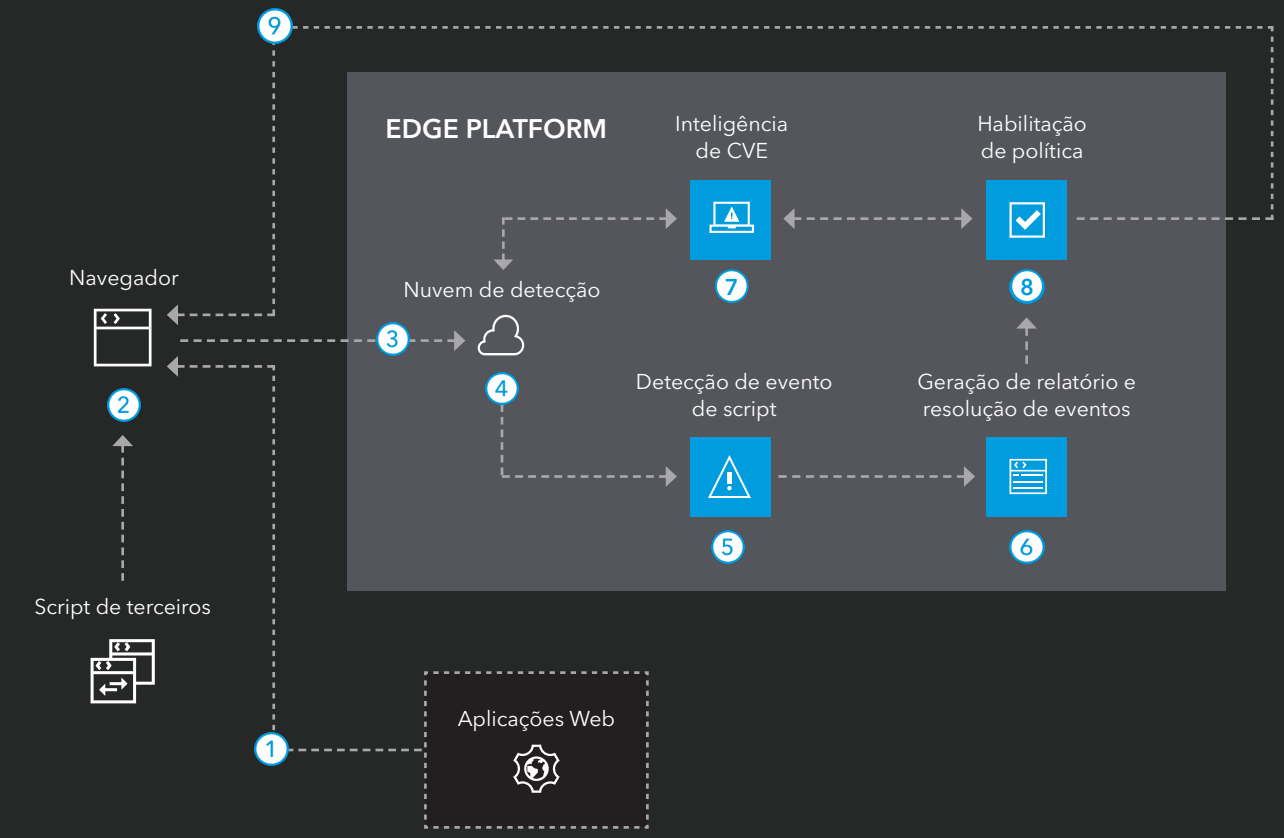


Fig. 2: A arquitetura do Page Integrity Manager

Do ponto de vista técnico, a detecção de bots e scripts é realizada por meio da injeção de JavaScript ou da integração do SDK (kit de desenvolvedor de software) de aplicações para dispositivos móveis, bem como por meio da análise coletada dos dados de rede, navegador e comportamento. O Bot Manager Premier analisa os dados para determinar se a atividade se originou de um bot ou de um ser humano, enquanto o Page Integrity Manager identifica todos os scripts injetados nas propriedades na Web. Qualquer atividade detectada de bot e script é categorizada como mal-intencionada ou não maliciosa, e as atividades mal-intencionadas são bloqueadas para evitar a exfiltração de dados.

Do ponto de vista da privacidade, a injeção de JavaScript e a integração do SDK são classificadas nas leis da UE como "tecnologia de cookies" e acionam a aplicação das leis de privacidade eletrônica. Além disso, alguns dos elementos de dados coletados, como o Endereço IP do usuário final, são classificados como dados pessoais e acionam a aplicação do GDPR.

Conformidade com as leis de privacidade eletrônica da UE

Para usar a tecnologia de cookies Bot Manager Premier e Page Integrity Manager de acordo com as leis de privacidade da UE, aplicam-se duas isenções das regras gerais: a isenção de consentimento e a do mecanismo de oposição. Com essas isenções, você pode implantar o Bot Manager Premier e o Page Integrity Manager em suas propriedades na Web para que operem imediatamente.

Aplicação da isenção de consentimento

Por padrão, a Diretiva de privacidade eletrônica requer a obtenção de consentimento do usuário final para o uso de qualquer tecnologia de cookies e coleta de dados relacionados. Somente quando o cookie for estritamente necessário para fornecer um serviço da sociedade da informação (em suas propriedades na Web), explicitamente solicitado por um assinante ou usuário (o usuário final), o consentimento de um indivíduo para o uso do cookie não é necessário e a tecnologia de cookie pode ser operada imediatamente.[3]

A maioria dos membros da UE espelhou esta exceção em suas leis locais de transposição da Diretiva de privacidade eletrônica.

A tecnologia de cookies usada no Bot Manager Premier e no Page Integrity Manager é necessária para a operação dos serviços. Sem a injeção de JavaScript, nenhum dado pode ser coletado e analisado e os bots ou os scripts não serão detectados e bloqueados. A finalidade da coleta de dados é a proteção dos dados pessoais fornecidos por meio de suas propriedades na Web contra comprometimento, exfiltração e violação. As autoridades locais responsáveis pela proteção de dados confirmaram que o uso da tecnologia de cookies para prevenção de fraudes e outros serviços de segurança se enquadra na isenção de consentimento.[4] A tabela a seguir mostra como o ICO (Information Commissioner's Office, escritório do comissário de informações) do Reino Unido descreve a aplicação da isenção de consentimento para os serviços de segurança.[5]

Atividade	É provável que atenda a uma isenção?
Segurança	**Depende da limitação de finalidade.** Os cookies primários usados para fins de segurança podem depender da isenção estritamente necessária; por exemplo, os cookies usados para detectar repetidas tentativas malsucedidas de login. Eles também podem durar mais tempo do que um cookie de sessão. No entanto, os cookies relacionados à segurança de outros serviços online, além dos seus, exigem consentimento. Isso ocorre porque a funcionalidade solicitada pelo usuário está relacionada ao seu serviço, e não aos de terceiros. Se você usar técnicas de impressão digital do dispositivo para uma finalidade de segurança específica, também poderá confiar na isenção estritamente necessária. No entanto, como ocorre com os cookies, se as informações forem processadas para fins secundários, como aqueles relacionados à segurança dos serviços online não solicitados pelo usuário, é necessário o consentimento. Isso também se aplica quando as informações são processadas para fins de prevenção de fraudes, especialmente nos casos em que vários serviços online usam um único serviço de prevenção de fraudes que processa informações de visitantes de todos esses serviços.

Aplicação da isenção de oposição

As leis de privacidade eletrônica exigem que as entidades ofereçam aos usuários finais um mecanismo para se opor à coleta de dados pela tecnologia de cookies. Esse requisito reflete o direito de se opor, de acordo com o Artigo 21 do GDPR.[6]

No entanto, há um caso extremo em que esse direito de controle será violado e exercer a oposição impedirá o desempenho das atividades de proteção de dados. Esse caso extremo se refere ao desempenho de um serviço de segurança baseado na tecnologia de cookies.

A oposição à tecnologia de cookies usada para detectar bots e scripts mal-intencionados interrompe os serviços de segurança que protegem contra o acesso não autorizado a dados pessoais. Desde que a tecnologia de cookies seja usada exclusivamente para fins de segurança, se o usuário ceder o controle sobre a coleta de dados para a tecnologia de cookies, não haverá danos aos direitos e à liberdade. Na verdade, conceder esse controle garante a operação contínua da tecnologia de cookies que protege os dados pessoais contra o acesso não autorizado.

Profissionais de privacidade em todo o mundo concordam com o requisito desta isenção de oposição: Quando um mecanismo de controle de dados oferecido a indivíduos (usuários finais) pode ser violado para permitir o acesso aos dados de maneira não autorizada, ele não tem finalidade e não deve ser colocado em prática. Em outras palavras, é de bom senso que uma operação simplificada de serviços de segurança de última geração prevaleça sobre a necessidade de oferecer um mecanismo de controle de dados (oposição) relacionado à tecnologia de cookies.[7]

Conformidade com a proteção de dados da UE

O Bot Manager Premier e o Page Integrity Manager processam dados em conformidade com o GDPR e outras leis aplicáveis de privacidade ou proteção de dados, incluindo o tipo de dados pessoais coletados e a finalidade da coleta.

Tipo de dados pessoais

O Bot Manager Premier e o Page Integrity Manager coletam dados de rede, navegador e comportamento, como sessão TCP, sessão TLS, ID da sessão, agente do usuário, cabeçalho da solicitação, URLs visitados, carimbo de data/hora, ENDEREÇO IP do usuário final, configurações do navegador e dados de localização geográfica de servidores edge, além de dados de comportamento, como toques na tela, movimentos do mouse e pressionamentos de teclas.

Finalidade

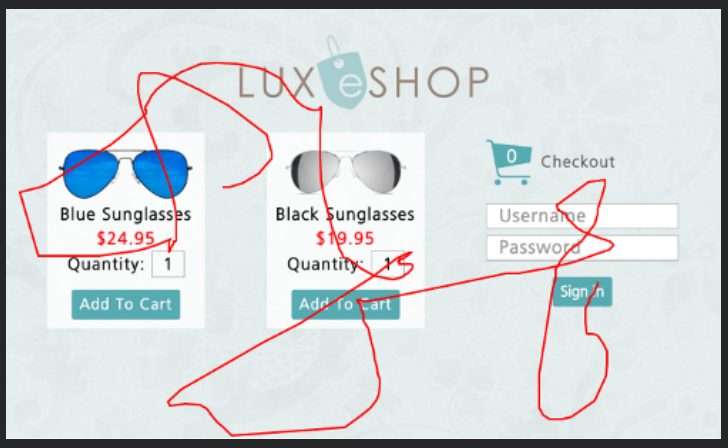
A finalidade da coleta e análise dos dados é a detecção de bots e scripts mal-intencionados que simulam o comportamento humano em suas propriedades na Web e a prevenção de exfiltração e violação de dados cometidas por eles.

Para isso, a Akamai analisa a maneira como um dispositivo é usado ao acessar suas propriedades na Web. A Akamai não identifica o usuário final ao realizar essa análise nem cria perfis de usuários finais. Além disso, os dados de comportamento coletados não são usados com o objetivo de identificar exclusivamente um indivíduo. Portanto, os dados não precisam ser categorizados como dados biométricos no GDPR.[8] Desse modo, não se tratam de dados confidenciais (em termos dos EUA) nem categorias especiais de dados (em termos da UE).

A Akamai coleta e analisa os dados de comportamento para determinar se sua propriedade na Web é acessada por um bot ou um ser humano, conforme descrito nas figuras abaixo.

Eventos do mouse

Exemplo de interação humana



Exemplos de bots

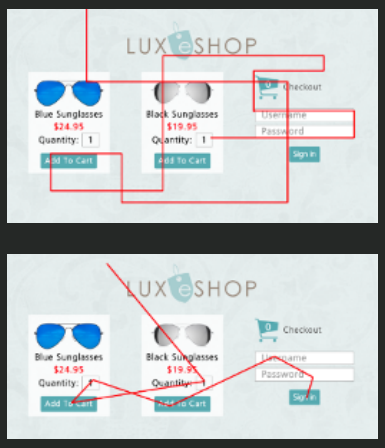
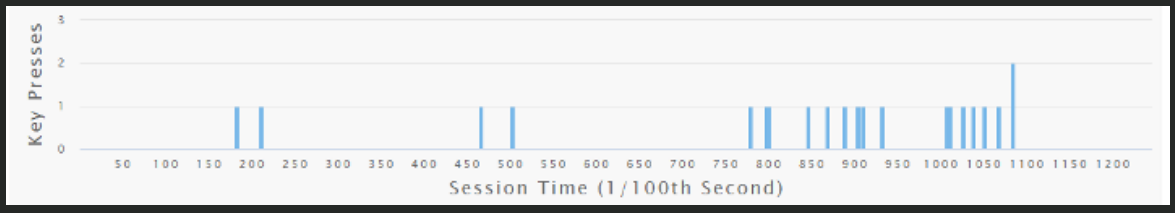


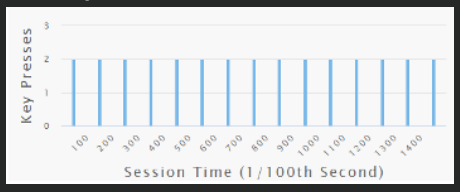
Fig. 3: Os bots sofisticados tentarão se esconder acionando movimentos do mouse. Isso foi projetado para emular a interação de um usuário. No entanto, após um determinado número de movimentos, um padrão emergirá. A Akamai pode detectar esses padrões para identificar um bot.

Detecção de padrão de pressionamento de teclas

Pressionamento de teclas por um ser humano



Exemplo de pressionamento de teclas por um bot



Exemplo de pressionamento de teclas por um bot

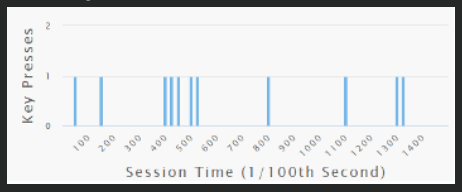


Fig. 4: Os seres humanos geralmente são mais aleatórios no pressionamento de teclas em comparação, até mesmo, com um bot sofisticado. Ao avaliar a velocidade e a cadência do pressionamento de teclas por um ser humano, a Akamai pode determinar se um usuário é um bot.

Base legal

A base legal para o processamento é o interesse legítimo da Akamai em fornecer serviços de segurança de informações e rede na forma de detecção e bloqueio de bots e scripts mal-intencionados. O interesse legítimo é uma base legal reconhecida para o desempenho dos serviços de segurança em conformidade com o GDPR.[9]

A Akamai entrega e protege até 30% de todo o tráfego da Internet. Sem os serviços de gerenciamento de bots e scripts dela, haveria muito mais exfiltração e violação de dados online prejudicando os direitos e a liberdade dos usuários finais.

Avaliação da necessidade e proporcionalidade

O processamento dos dados é necessário para que os serviços de segurança de informações e rede da Akamai sejam considerados de última geração de acordo com as leis de privacidade. Ao realizar a análise dos dados de rede, navegador e comportamento coletados, a Akamai pode determinar precisamente as ações e os scripts de bots ou humanos injetados em uma propriedade na Web.

A análise de todos os elementos de dados coletados é proporcional, considerando a sofisticação dos bots e scripts atuais. A redução da coleta de dados afeta a precisão da análise, resultando em uma detecção menos eficaz de atividades mal-intencionadas. Os bots não podem ser detectados analisando apenas Endereços IP do usuário final. Embora os detalhes do navegador e da rede indiquem o uso do dispositivo, eles estão limitados a mecanismos passivos baseados em assinatura e propensos a altos falsos positivos e falsos negativos. A segurança de última geração para propriedades na Web[10] se estende à sofisticada detecção de bots. Os bots ativos que simulam o comportamento humano são detectados somente onde os dados de comportamento são analisados.

A coleta de mais dados seria excessiva, pois a análise não melhoraria.

Avaliação de riscos

O risco para os direitos e as liberdades dos usuários finais associados às atividades de processamento do Bot Manager Premier e do Page Integrity Manager é baixo. Os dados de navegador, rede e comportamento não são categorizados como altamente confidenciais, sigilosos ou uma categoria especial de dados pessoais.[11] As atividades de processamento da Akamai relacionadas ao Bot Manager Premier e ao Page Integrity Manager estão descritas na Declaração de privacidade da Akamai e são transparentes para as partes interessadas. A Akamai está em conformidade com o princípio de minimização de dados, coletando apenas os dados necessários para detecção de bots e JavaScript.

A Akamai aplica medidas técnicas e organizacionais adequadas para proteger os dados pessoais processados contra o acesso não autorizado de terceiros. Essas medidas também são publicadas de forma transparente em nosso website: Programa de Segurança da informação da Akamai e Medidas técnicas e organizacionais da Akamai.

A análise para a detecção de bots e scripts é realizada em sistemas Akamai implantados nos Estados Unidos. Portanto, onde os usuários finais da UE estão acessando propriedades na Web protegidas pelo Bot Manager Premier e pelo Page Integrity Manager, a análise requer o processamento de dados pessoais da UE nos Estados Unidos. Para garantir a proteção adequada dos dados quando processados nos Estados Unidos, a Akamai implementou as Cláusulas contratuais padrão da UE no grupo Akamai, com nossos clientes e subprocessadores, e implementou proteções técnicas adicionais para proteger os dados pessoais quando processados nos Estados Unidos contra acesso de terceiros.

A Akamai aplica o mesmo requisito de proteção de dados a todas as suas entidades de grupo, independentemente da localização da entidade da Akamai. Colocamos em prática medidas complementares para proteger os dados transferidos contra o acesso de terceiros. Além disso, na visão da Akamai, os dados transferidos para os Estados Unidos pela Akamai para o Bot Manager Premier e o Page Integrity Manager não são o tipo de dados que as agências de vigilância de dados (EUA) estão interessadas ao realizar suas operações de vigilância.[12] A maioria dos dados é livremente acessível como requisito para estabelecer uma conexão com a Internet, e um terceiro não precisa abordar a Akamai para coletar os dados em questão. Há muitas outras formas mais convenientes de acesso a esses dados por terceiros. Portanto, a Akamai avaliou que os riscos de acesso de terceiros aos dados transferidos para os Estados Unidos para o Bot Manager Premier e o Page Integrity Manager são mínimos. Os detalhes estão descritos na Declaração de transferência de dados da Akamai no Privacy Trust Center da Akamai.

Em conformidade com o princípio de minimização e segurança dos dados, a Akamai definiu o período de retenção para 90 dias. Esse período é apropriado considerando a necessidade de analisar os dados de rede, navegador e comportamento em um determinado período entre as regiões, para permitir a detecção mais eficaz de bots e scripts.

Os serviços de detecção e gerenciamento de bots e scripts que a Akamai oferece não apenas protegem suas propriedades na Web, mas também melhoram o estado da Internet em geral. Ao detectar e bloquear bots e scripts na Intelligent Edge Platform da Akamai, não só evitamos a exfiltração e a violação de seus dados pessoais de usuário final, como também ganhamos inteligência contra ameaças para os serviços de rede e segurança beneficiando milhões de usuários finais.

Medidas de mitigação

Quando a Akamai identificou um risco para os direitos e a liberdade do titular dos dados pela operação dos serviços Bot Manager Premier e Page Integrity Manager, ela atenuou esses riscos. Ao coletar os dados de comportamento, o usuário final não é identificado. Além disso, a Akamai protegeu adequadamente os dados pessoais e colocou em prática medidas complementares para garantir que os dados transferidos sejam devidamente protegidos contra o acesso de terceiros.

Resumo

O Bot Manager Premier e o Page Integrity Manager da Akamai estão em conformidade com as leis de proteção de dados da UE. A tecnologia de cookies utilizada para o funcionamento dos serviços é estritamente necessária e permite a proteção dos dados pessoais do usuário final; portanto, as isenções do requisito de consentimento e do mecanismo de oposição se aplicam.

A coleta de dados necessária para operar os serviços é legítima, necessária e proporcional. Além disso, as medidas de mitigação tomadas garantem que o risco de atividades de processamento seja muito baixo para os direitos e a liberdade dos usuários finais. Os benefícios do desempenho do Bot Manager Premier e do Page Integrity Manager para seus usuários finais e outros indivíduos online superam os riscos, já que todos se beneficiam de uma Internet mais segura.

Akamai Technologies
Dra. Anna Schemits, DPO EMEA

Fontes:

1. As declarações aqui contidas também se aplicam ao Service Bot Manager Standard da Akamai, exceto pelo escopo da coleta de dados, que se limita aos dados de rede e do navegador. Saiba mais sobre o Bot Manager da Akamai: https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. Consulte "Privacidade digital", disponível em: https://ec.europa.eu/digital-single-market/en/online-privacy
3. Consulte a emenda do Artigo 5 (3) da Diretiva de privacidade eletrônica 2002/58/CE pela Diretiva 2006/24/CE, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.
4. Veja, por exemplo, as diretrizes de cookies do ICO do Reino Unido, disponíveis em 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, as diretrizes da CNIL francesa, disponíveis em https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines, ou as diretrizes da Comissão das autoridades alemãs (somente em alemão), disponíveis em https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
5. Consulte as diretrizes de cookies de ICP, disponível em: 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. Consulte o Artigo 21 (1) do GDPR, disponível em: https://gdpr-info.eu/art-21-gdpr/.
7. Veja, por exemplo, as diretrizes do ICO, disponível em: 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 o Artigo 9 (1) do GDPR, disponível em: https://gdpr-info.eu/art-9-gdpr/.
9. Consulte o Preâmbulo 49 do GDPR, disponível em: https://gdpr-info.eu/recitals/no-49/
10. Conforme exigido pelo Artigo 32 do GDPR, disponível em: https://gdpr-info.eu/art-32-gdpr/
11. Consulte o Artigo 9 do GDPR, disponível em: https://gdpr-info.eu/art-9-gdpr/
12. Proteções de privacidade dos EUA relevantes para SCCs e outras bases legais da UE para Transferências de dados entre UE e EUA após o Schrems II, setembro de 2020. Disponível em: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A Akamai Intelligent Edge Platform engloba tudo, desde a empresa até a nuvem, para que os clientes e suas empresas possam ser rápidos, inteligentes e estar protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a obter vantagem competitiva por meio de soluções ágeis que estendem o poder de suas arquiteturas multinuvem. A Akamai mantém as decisões, as aplicações e as experiências mais próximas dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções Edge Security, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeos da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante o ano todo. Para saber por que as principais marcas do mundo confiam na Akamai, visite **www.akamai.com**, **blogs.akamai.com** ou siga **@Akamai** no Twitter. Nossas informações de contato globais podem ser encontradas em **www.akamai.com/locations**. Publicado em 03/21.