设计中考虑隐私

Akamai Bot Manager Premier 和 Page Integrity Manager 服务如何满足欧盟隐私要求？

概览

Akamai 深知，要让客户信任我们的技术和服务，保护个人数据和遵守隐私要求至关重要。本白皮书概述了 Bot Manager Premier[1] 和 Page Integrity Manager 如何满足《欧盟电子隐私指令》和《通用数据保护条例》(GDPR)[2] 的要求，以帮助您评估运营这些服务所面临的风险。

Bot Manager Premier 旨在检测由爬虫程序（机器人）生成的、针对您的 Web 资产的自动访问请求，这些爬虫程序会模仿人类行为，以收集和利用最终用户的登录数据。Page Integrity Manager 可以检测出于滥用目的而注入到这些资产中的 JavaScript。一旦检测到爬虫程序和脚本，Akamai 就会根据您的指示、常识和我们的威胁情报，将它们划分为非恶意和恶意活动。恶意活动将被阻止，只有非恶意的爬虫程序和脚本才能访问您的源站服务器、基础架构和数据。

这两项服务都能确保最终用户提供的个人数据不被泄露和滥用。British Airways 和 The North Face 最近经历的安全和数据泄露事件证明了防范此类威胁的重要性。

Bot Manager Premier 架构

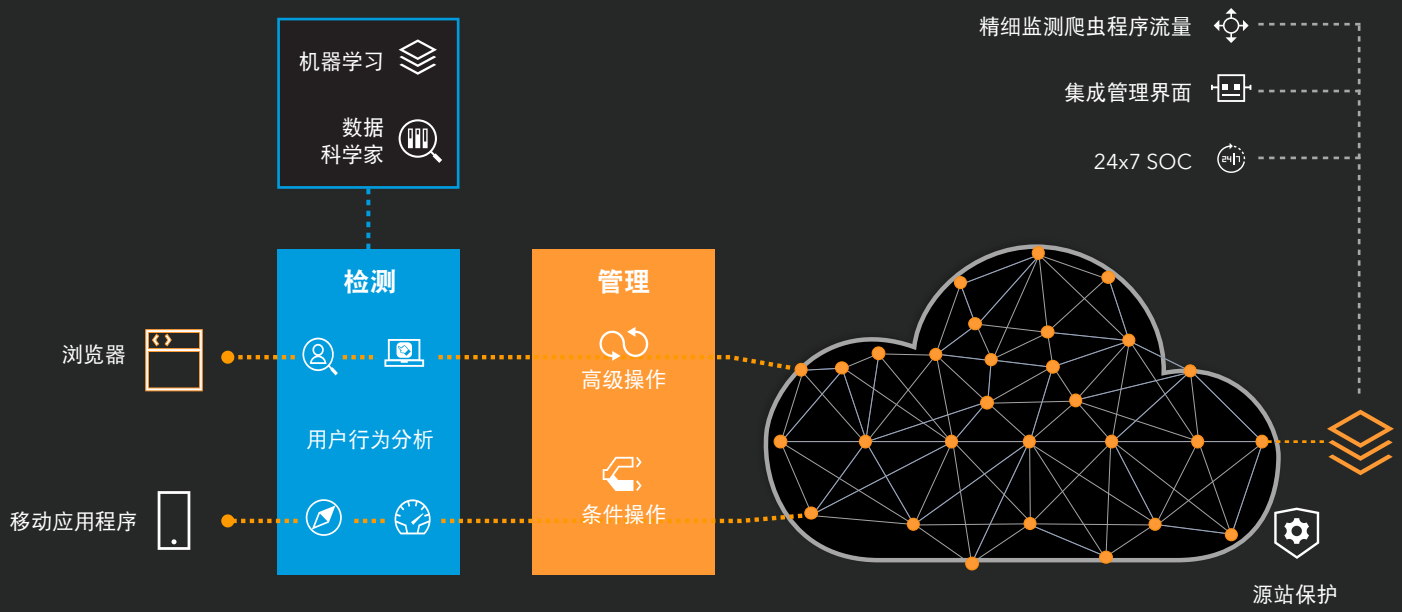


图 1：Bot Manager Premier 架构

Page Integrity Manager 架构

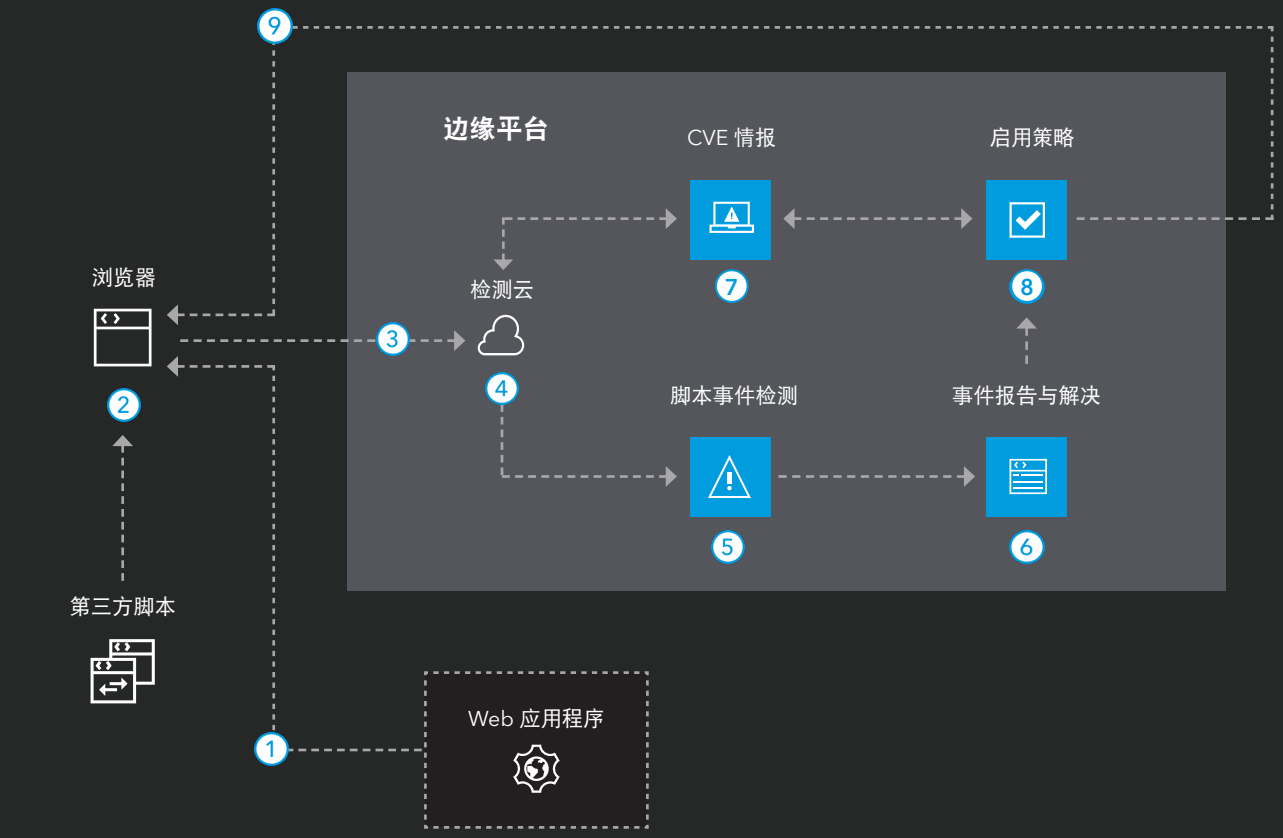


图 2：Page Integrity Manager 架构

从技术角度来看，在执行爬虫程序和脚本检测时，借助的是 JavaScript 注入或移动应用程序软件开发人员工具包 (SDK) 集成，且在此过程中收集了针对网络、浏览器和行为数据的分析数据。Bot Manager Premier 可分析数据，以确定活动是来自爬虫程序还是人类，Page Integrity Manager 则可以识别所有注入 Web 资产的脚本。随后，任何检测到的爬虫程序和脚本活动都会被归类为恶意活动或非恶意活动，恶意活动会被阻止，以避免数据泄露。

从隐私的角度来看，JavaScript 注入和 SDK 集成在欧盟法律下被归为“Cookie 技术”，因此需遵守电子隐私法。此外，收集的一些数据元素（比如最终用户的 IP 地址）被归类为个人数据，因此需遵守 GDPR。

遵守欧盟电子隐私法

在根据欧盟隐私法使用 Bot Manager Premier 和 Page Integrity Manager Cookie 技术时，可应用针对一般规则的两项豁免原则：同意豁免和选择退出机制豁免。这些豁免允许您将 Bot Manager Premier 和 Page Integrity Manager 放在您的 Web 资产上，并立即运行。

同意豁免原则的适用情况

默认情况下，《电子隐私指令》要求您在使用任何 Cookie 技术和相关数据收集时，必须获取最终用户的同意。只有当绝对需要使用 Cookie 来提供订户或用户（最终用户）明确请求获取的信息社会服务（位于您的 Web 资产上）时，才不需要获取个人对 Cookie 用途的同意，此时，Cookie 技术可以立即运行。[3]

大多数欧盟成员国/地区将这一例外情况纳入到了《电子隐私指令》在其当地的同等法律中。

Bot Manager Premier 和 Page Integrity Manager 使用的 Cookie 技术对于服务的运行必不可少。如果没有 JavaScript 注入，就无法收集和分析数据，也无法检测和阻止爬虫程序或脚本。收集数据的目的是为了防止通过您的 Web 资产提供的个人数据遭到泄露、渗透和滥用。当地数据保护机关确认，使用 Cookie 技术提供防欺诈功能和其他安全服务属于同意豁免的范畴。[4] 下表概述了英国信息专员办公室 (ICO) 对于安全服务同意豁免原则的适用性。[5]

活动	可能适用于豁免原则?
安全性	**取决于用途限制。** 用于保障安全的第一方 Cookie 可以应用绝对必要的豁免；例如，用于检测反复失败的登录尝试的 Cookie。它们的持续时间也可以比会话 Cookie 更长。 但是，除了您自己的服务外，与其他在线服务的安全功能有关的 Cookie 需要征得用户同意。这是因为，用户请求的功能与您的服务（而不是其他任何服务）有关。 如果您出于特定的安全目的使用设备指纹技术，则您也可以应用绝对必要的豁免。但是，与 Cookie 一样，如果信息的处理是出于次要目的 - 例如，与用户未请求的在线服务的安全性有关的目的 - 则需要征得用户同意。 此原则也适用于为防止欺诈而对信息进行处理的情况，特别是当多个在线服务使用单个防欺诈服务来处理所有这些服务的访问者信息时。

选择退出豁免原则的适用性

电子隐私法要求机构为最终用户提供一种机制，以选择拒绝通过 Cookie 技术收集数据。此要求反映了 GDPR 第 21 条规定的拒绝权。[6]

但是存在一种非常特殊的情况，在这种情况下，此控制权会被滥用，执行的选择退出操作会妨碍开展数据保护活动。这种非正常情况指的是运行基于 Cookie 技术的安全服务。

选择停用用于检测恶意爬虫程序和脚本的 Cookie 技术后，会停止相关的安全服务，导致无法防止攻击者未经授权访问个人数据。只要 Cookie 技术仅用于安全目的，那么，哪怕最终用户无法控制 Cookie 技术执行的数据收集，也不会对用户的权利和自由造成损害。相反，正是由于缺乏控制，才确保了 Cookie 技术的持续运行，从而保护个人数据不会遭受未经授权的访问。

世界各地的隐私专家都同意这项选择退出豁免要求：如果提供给个人（最终用户）的数据控制机制可能被滥用，导致攻击者能够以未经授权的方式访问数据，那么，数据控制机制就没有任何意义，必须避免实施这种机制。换句话说，从常理上讲，相比提供与 Cookie 技术有关的数据控制（选择退出）机制的需求，更重要的是确保先进安全服务的流畅运行。[7]

欧盟数据保护合规性

Bot Manager Premier 和 Page Integrity Manager 根据 GDPR 和其他适用的数据保护或隐私法处理数据，包括收集的个人数据类型和收集目的。

个人数据类型

Bot Manager Premier 和 Page Integrity Manager 会收集网络、浏览器和行为数据，比如 TCP 会话、TLS 会话、会话 ID、用户代理、请求标头、访问的 URL、时间戳、最终用户 IP 地址、浏览器设置和边缘服务器的地理位置数据，以及行为数据，比如屏幕触摸、鼠标移动和按键操作。

目的

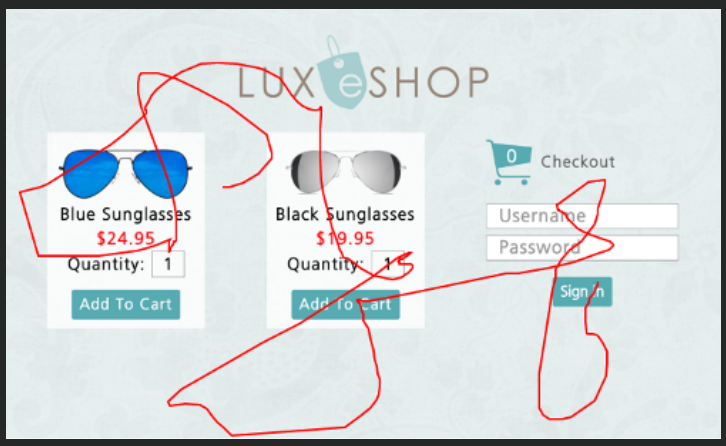
收集和分析数据的目的是检测您的 Web 资产中可模仿人类行为的恶意爬虫程序和脚本，并防止它们执行数据渗透和滥用。

为了达到此目的，Akamai 会分析设备在访问您的 Web 资产时的使用方式。在进行此分析时，Akamai 不会识别最终用户的身份，也不会创建最终用户的档案。此外，收集的行为数据不会用于唯一标识个人的身份。因此，根据 GDPR 的规定，这些数据不需要被归类为生物识别数据。[8] 因此，它既不是敏感数据（按照美国的说法），也不是特殊的数据类别（按照欧盟的说法）。

Akamai 将收集和分析行为数据，以确定访问您的 Web 资产的是爬虫程序还是人类，如下图所示。

鼠标活动

人类示例



爬虫程序示例

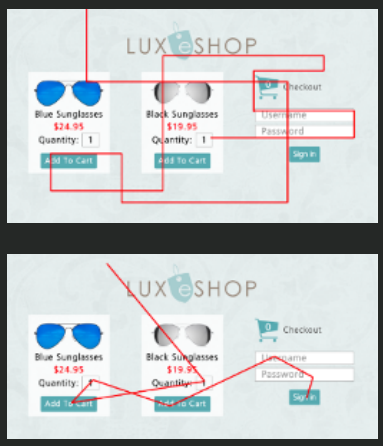
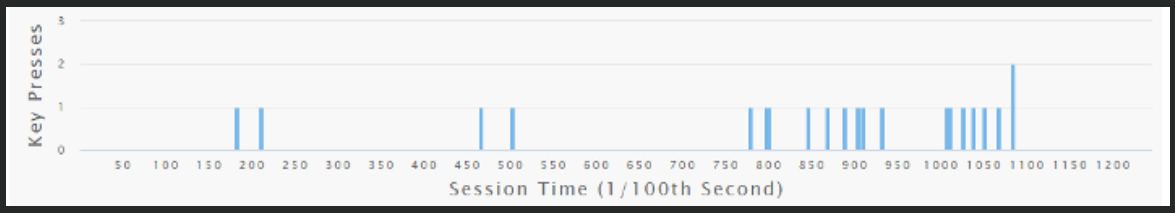


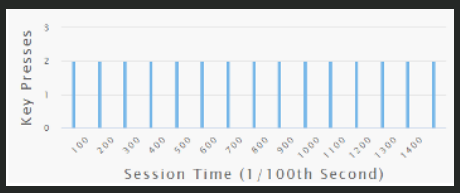
图 3：复杂的爬虫程序会试图通过触发鼠标移动来隐藏自身。这是为了模拟用户的交互。但是，在一定数量的移动之后，会出现一种模式。Akamai 可以检测这些模式以识别爬虫程序。

按键模式检测

人类按键操作



爬虫程序按键示例



爬虫程序按键示例

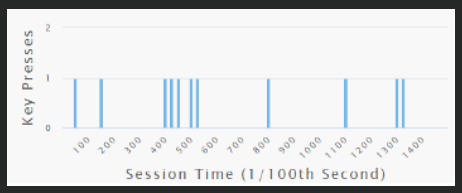


图 4：人类的按键模式通常比复杂的爬虫程序更加随机。通过检查人类按键的速度和节奏，Akamai 可以进一步确定用户是否是爬虫程序。

法律依据

此数据处理的法律依据在于 Akamai 拥有正当权益来检测及阻止恶意爬虫程序和脚本，进而提供网络与信息安全服务。根据 GDPR，合法权益是执行安全服务的公认法律依据。[9]

Akamai 交付并保护整个互联网中高达 30% 的流量。如果它没有提供爬虫程序和脚本管理服务，将会出现更多的在线数据渗透和数据滥用，从而损害最终用户的权利和自由。

必要性和相称性评估

为了使 Akamai 的网络和信息安全服务达到隐私法规定的先进水平，必须对数据进行处理。通过对收集到的网络、浏览器和行为数据进行分析，Akamai 可以精确地确定爬虫程序或人类的操作以及注入 Web 资产的脚本。

考虑到如今爬虫程序和脚本的复杂程度，对所有收集的数据元素执行的分析都具有相应的必要性。减少数据收集会影响分析的准确性，导致对恶意活动的检测效果降低。只分析最终用户的 IP 地址的话，将无法检测爬虫程序。虽然浏览器和网络详细信息表明了设备的使用情况，但它们局限于被动的、基于签名的机制，而且容易出现较高的误报率和漏报率。先进的 Web 资产安全功能[10] 还包括复杂的爬虫程序检测。只有在分析行为数据后，才可检测出模仿人类行为的活跃爬虫程序。

没有必要收集更多的数据，因为分析效果不会提高。

风险评估

Bot Manager Premier 和 Page Integrity Manager 的处理活动对终端使用者的权利和自由仅会造成少量风险。浏览器、网络和行为数据没有被归类为高度机密、敏感或特殊类别的个人数据。[11] 在 Akamai 的隐私声明中介绍了与 Bot Manager Premier 和 Page Integrity Manager 相关的 Akamai 处理活动，可供相关方随时查阅。Akamai 遵守数据最低程度收集原则，只收集爬虫程序和 JavaScript 检测所需的数据。

Akamai 采取了适当的技术和组织措施，以确保处理的个人数据不被第三方未经授权访问。此类措施也会在我们的网站上公布：Akamai 的信息安全计划和 Akamai 的技术和组织措施。

爬虫程序和脚本检测的分析在美国部署的 Akamai 系统上进行。因此，当欧盟最终用户访问受 Bot Manager Premier 和 Page Integrity Manager 保护的 Web 资产时，分析过程需要在美国处理欧盟个人数据。为了确保在美国处理数据时能够提供充分保护，Akamai 已经在 Akamai 集团内部与我们的客户和子处理商制定了欧盟标准合同条款，并实施了额外的技术保障措施，以防止在美国处理的个人数据遭到第三方访问。

无论 Akamai 实体位于何处，Akamai 对其所有集团附属实体都应用了同样的数据保护要求。我们已经制定了补充措施，以保护传输的数据不被第三方访问。此外，在 Akamai 看来，Akamai 为 Bot Manager Premier 和 Page Integrity Manager 传输到美国的数据并不是（美国）监管机构在执行监管行动时感兴趣的数据类型。[12] 大多数数据都可以被自由访问，因为这是建立互联网连接的必要条件，而第三方不需要联系 Akamai 以收集这些数据 - 第三方要想访问这些数据，还有许多更加方便的方法。因此，Akamai 经过评估得出结论，传输到美国的 Bot Manager Premier 和 Page Integrity Manager 数据遭到第三方访问的风险非常小。Akamai 隐私信任中心内的 Akamai 数据传输声明中概述了相关详情。

根据数据最低程度收集和数据安全原则，Akamai 将保留期设置为 90 天。考虑到需要对一定时期内跨区域的网络、浏览器、行为数据进行分析，以实现有效的爬虫程序和脚本检测，此保留期非常合适。

Akamai 提供的爬虫程序和脚本检测与管理服务不仅能保证您的 Web 资产安全，还能改善互联网的整体状况。通过在 Akamai Intelligent Edge Platform 上检测和阻止爬虫程序及脚本，我们不仅可以防止您的最终用户个人数据遭到渗透和滥用，还可以获得网络和安全服务的威胁情报，使数百万最终用户受益。

缓解措施

当 Akamai 发现 Bot Manager Premier 和 Page Integrity Manager 服务的运行会对数据主体的权利和自由造成风险时，它会缓解这些风险。在收集行为数据时，不会识别最终用户的身份。此外，Akamai 还对个人数据进行了适当保护，并制定了补充措施，以确保传输的数据拥有足够的安全性，以防止第三方访问。

总结

Akamai Bot Manager Premier 和 Page Integrity Manager 符合欧盟数据保护法。服务运营所使用的 Cookie 技术是绝对必要的，并且能够保护最终用户的个人数据，因此，同意要求和选择退出机制的豁免原则在这里适用。

运营服务所需的数据收集合法、必要且符合比例要求。此外，采取的缓解措施可确保尽可能降低处理活动对最终用户的权利和自由造成的风险。通过运行 Bot Manager Premier 和 Page Integrity Manager，您的最终用户和其他在线用户收获的好处超过了风险，因为每个人都能通过更安全的互联网获益。

Akamai Technologies
Anna Schmits 博士，EMEA DPO

来源：

1. 本文所做的声明也适用于 Akamai 服务 Bot Manager Standard（数据收集范围除外，该范围仅限于网络和浏览器数据）。详细了解 Akamai Bot Manager：https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. 要了解“数字化隐私”，请访问：https://ec.europa.eu/digital-single-market/en/online-privacy 。
3. 请参阅 2006/24/EC 号指令对 2002/58/EC 号电子隐私指令第 5 (3) 条的修订，网址为：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN 。
4. 例如，请参阅英国 ICO 的 Cookie 准则，网址为 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、法国 CNIL 的准则，网址为 https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines，或德国当局委员会的准则（仅提供德语版本），网址为 https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf。
5. 参阅 ICP 的 Cookie 指南，网址为 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. 参阅 GDPR 第 21 (1) 条，网址为：https://gdpr-info.eu/art-21-gdpr/ 。
7. 例如，请参阅 ICO 的指导意见，网址为：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. 参阅 GDPR 第 9 (1) 条，网址为：https://gdpr-info.eu/art-9-gdpr/ 。
9. 参阅 GDPR 第 49 条释义，网址为：https://gdpr-info.eu/recitals/no-49/
10. 根据 GDPR 第 32 条的要求，网址为：https://gdpr-info.eu/art-32-gdpr/
11. 参阅 GDPR 第 9 条，网址为：https://gdpr-info.eu/art-9-gdpr/
12. Schrems II 法案后适用于欧盟向美国的数据转移、与 SCC 和其他欧盟法律依据相关的美国隐私保障措施，2020 年 9 月。网址为：https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Akamai *Intelligent Security Starts at the Edge*

Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其公司获得快速、智能且安全的体验。全球优秀品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而获得竞争优势。Akamai 使决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均由优质客户服务、分析和全天候监控提供支持。如需了解全球顶级品牌信赖 Akamai 的原因，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。您可访问 www.akamai.com/locations 查找全球联系信息。 发布时间：2021 年 3 月。

扫码关注・获取最新 CDN 前沿资讯