CLOUDFLARE

解决方案简介

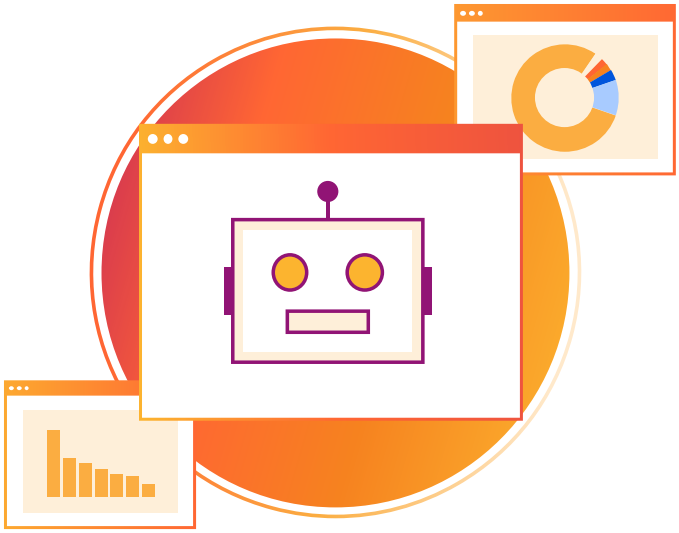
管理恶意机器人的四种策略

避免无用机器人造成高昂损失和收入下降

互联网上机器人无处不在

现代互联网上机器人很常见，因为它们有助于重要任务的自动化。据估计，互联网总流量的 40-50% 由机器人驱动，其中许多机器人正在执行合法的业务功能。

然而，机器人也经常被犯罪分子用来攻击 Web 资产，并造成代价高昂的损害。恶意机器人可窃取数据，入侵用户账户，通过在线表单提交垃圾数据，并进行其他恶意活动。这些恶意机器人会浪费宝贵的计算和站点资源，窃取数据，扭曲流量分析。



什么是机器人管理？

机器人管理是指阻止无用或恶意机器人流量，同时允许有用的机器人访问 Web 资产。其做法是检测机器人活动，识别有用和无用的机器人行为，并识别无用活动的来源。

这为什么重要？

机器人管理非常必要，因为如果不加以控制，机器人有可能造成严重和代价高昂的问题。在对到达其 Web 资产的任何恶意机器人流量进行屏蔽时，组织需要确保没有拦截必要的机器人，例如搜索引擎爬虫。

可以采取什么措施？

在恶意机器人发起攻击之前进行识别和阻止是任何完善安全策略的关键组成部分。我们分享了四个真实 Cloudflare 客户的案例，这些客户使用 Cloudflare 产品，通过四种不同的策略解决了他们的机器人管理挑战。

阻止机器人

这种方法需要谨慎，因为许多合法的业务流程，如搜索引擎索引，要求机器人能够访问公司资源。

阻止机器人		
挑战	**解决方案**	**结果**
某在线游戏公司注意到用户投诉显著增加。他们的账户遭到黑客入侵，信用卡信息被盗。恶意行为者正在使用自动化机器人来暴力破解登录凭据，获得用户帐户的访问权限，并最终接管它们。	安全团队采用了**速率限制**和高级 **Bot Management** 技术，检测短时间内多次尝试登录的行为。检测到异常行为时，速率限制会开始自动阻止恶意请求。自从实施速率限制功能以来，该公司就再未遭受过任何凭据填充攻击。	所有公司都需要在严格的安全与最佳用户体验之间取得平衡。 正确的工具组合可以帮助检测和防止恶意机器人流量，同时尽量减少误报和对真实用户的障碍。

减慢攻击者的节奏

这种技术最大程度增加对所有可疑网络请求的响应时间。

减慢攻击者的节奏		
挑战	**解决方案**	**结果**
一家体育博彩公司注意到交易大幅减少。 经过分析，他们发现有恶意机器人活动在他们的网站上抓取赔率数据，并利用这些信息来获得竞争优势。	该公司没有阻止机器人，因为恶意行为者会绕过此类拦截措施。取而代之，他们减慢了下注的数据获取。 **他们使用 Headers Override** 根据 **Bot Management** 分析标记可疑请求，然后使用 **Workers** 脚本来响应这些请求并减慢其速度。	这个方法允许该公司恢复正常用户活动。其他方法包括对高频请求启用 CAPTCHA 验证码或定期修改 HTML 标记。 这些做法会阻断机器人工作流，从而使持续的内容抓取变得更加复杂。

欺骗机器人

尽管很多公司部署了机器人对策，但目标坚定的攻击者仍能绕过有关措施。取而代之，一些公司决定进行反击。

欺骗机器人		
挑战	**解决方案**	**结果**
一家体育博彩公司尝试找到一种解决方案，对付从其网站抓取赔率的机器人。 经过一番考虑，他们决定使用多个 Cloudflare 产品推出一种变通方案，向机器人提供随机化的信息。	当系统监测到某个请求来自恶意机器人时，就会接受请求并产生一个新的工作流： 请求 → **WAF** (发现机器人) → **Bot Management**(分配威胁评分) → **Workers** (产生随机化数据) → **Workers** (向机器人返回随机化数据)	这个新工作流生成了新的随机数据，并将其返回给恶意机器人。 因此，旨在抓取赔率并造成损害的机器人只能获得一些无用的信息，这抑制了进一步的滥用。

进行动态分析

随着机器人变得越来越复杂，公司需要收集关于机器人的数据并进行动态分析，然后再采取行动。这些目标可能包括检测恶意注册、赔率、奖金索取等。为了确保彻底分析，安全团队可能需要结合来自内部和外部工具的多个数据源，以分析机器人流量的参数。

进行动态分析		
挑战	**解决方案**	**结果**
某博彩公司启动一场营销活动，以注册奖励吸引新用户。活动开始不久后，他们就注意到有机器人在进行虚假注册。 该公司已经有一些内部分析工具，但这些工具未能提供机器人行为的全面信息。	该团队部署了 Cloudflare 的高级 **Bot Management**（含 JA3 特征）为发送到注册页面的所有互联网流量生成**原始日志**。他们通过引入机器人评分和 JA3 特征充实了内部系统，使其能够更清晰地识别机器人。	经过深入分析，该公司得以取消虚假注册，避免了夸大新获得用户的统计数据。 他们将使用 JA3 特征的常规机器人分析纳入其最佳实践。

比恶意机器人领先一步

Cloudflare Bot Management

简单部署
无需复杂配置或维护

低延迟
延迟中位数 <0.3 毫秒

丰富分析
将流量日志与其他数据源（如 SIEM 或 BI 工具）相关联

精确控制
调优规则，使用可视化规则构建器，或编写自己的模式匹配规则

防止恶意机器人损害您的业务

机器人正在变得越来越先进。随着攻击者的手段日益复杂，机器人检测和拦截存在固有的局限性。当今企业需要不断调整策略，以应对攻击者的工具更新，同时在强大的安全性和尽量减少用户摩擦之间实现适当的平衡。

无论决定使用什么策略，都要确保合作伙伴有一套灵活的工具来有效地管理机器人。要进一步了解 Cloudflare 能如何帮助您应对机器人的挑战，请联系我们以获得个性化评估。

值得您信赖的情报

Cloudflare 代理约 20% 的全球互联网流量，就 Cloudflare 网络中的恶意机器人行为提供了广泛的实时情报。
此外，Cloudflare 还与多个合作伙伴合作，共享有关被盗登录凭据的情报，从而更容易在遭到入侵前发现帐户接管尝试。

开启通往更快、更可靠、更安全网络的旅程。

预约咨询

尚未准备好进行评估？

进一步了解 Cloudflare