Cloudflare Bot Management

无需验证码即可阻止恶意机器人并管理 AI 机器人。

机器人潜藏在您的流量中。恶意机器人会损害收入与用户体验。

互联网上 **30%** 的应用流量是自动化流量[1]。基于地理位置和 IP 地址的启发式算法以及 CAPTCHA 验证等传统防御手段都很容易被现代机器人绕过。这些（措施）也会对真实用户造成很大困扰。

凭借对全球**约 20%** Web 流量的可见性，在对 AI 爬虫与搜索机器人的指纹识别方面，没有任何平台能超越 Cloudflare[2]。

Cloudflare Bot Management 帮助组织管理 Web 、移动应用的 AI 爬虫和机器人流量，而无需使用 CAPTCHA 验证码。允许经过验证的机器人和合规的 AI 爬虫访问应用，同时阻止不合规的 AI 机器人和恶意机器人。这是我们应用安全产品组合中的一项关键功能。

产品优势

- 防止欺诈、经济损失和品牌受损
- 提升 Web 和移动应用体验
- 有效阻止不必要的 AI 爬虫和搜索机器人

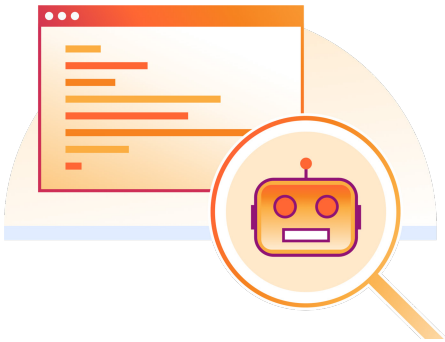

图 1： Cloudflare Bot Management 集成于我们的应用安全产品组合中

来源

1. Cloudflare Radar 数据，2024 年
2. W3techs，反向代理服务的使用统计和市场份额，2025 年

Cloudflare Bot Management 如何工作

Cloudflare 将来自全球和应用特定机器学习、客户端 JavaScript、移动设备和启发式算法等多种来源的多层检测结果整合起来，为每个 HTTP 请求生成统一的机器人评分。这个机器人评分指示该请求来自机器人的可能性。这个机器人评分用于诸如阻止或允许之类的标准响应，以及通过其他 Cloudflare 产品实现的自定义响应策略。机器人分析，包括机器人评分、HTTP 请求元数据等，可在 Cloudflare 仪表板用户界面中或通过第三方工具中的 Cloudflare API 获取。

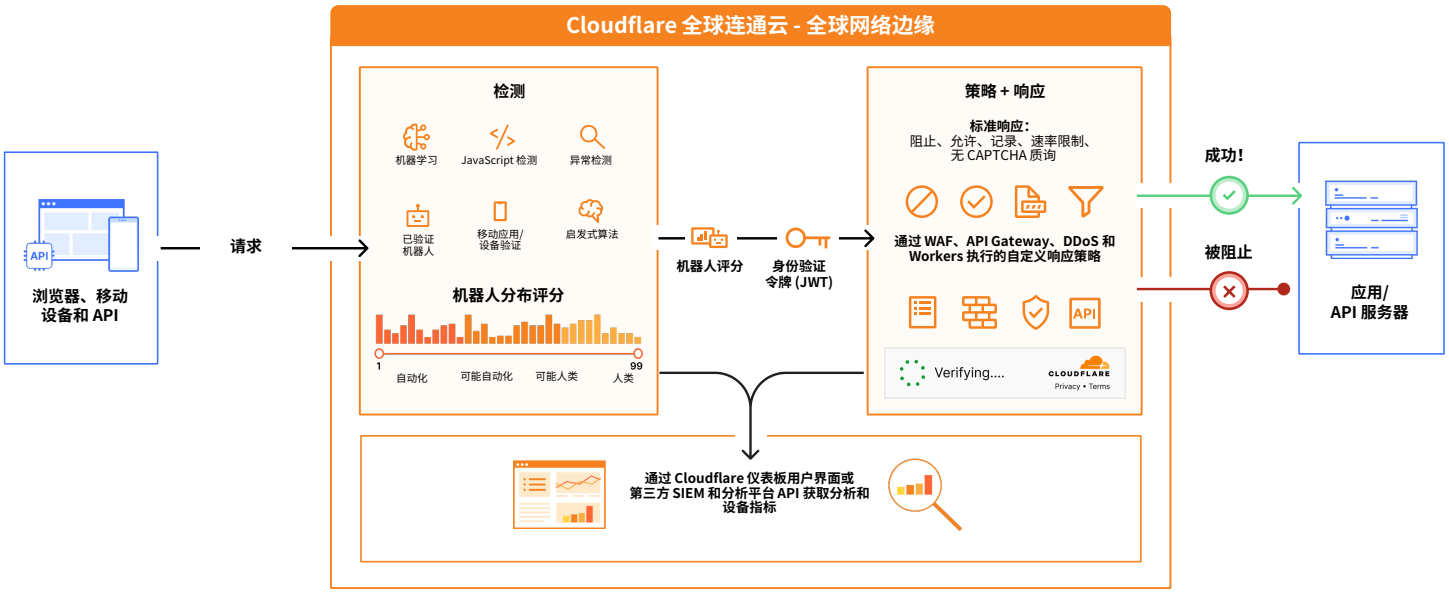

图 2：通过 Cloudflare Bot Management 的请求路径示例

Cloudflare Bot Management 的主要功能

帐户接管和滥用

基于机器学习的模型能够在公开披露前检测出漏洞，从而有效防范 zero-day 漏洞。防御破纪录的 DDoS 攻击，保护敏感数据，降低客户端风险，并监控 Web 应用的软件供应链。

防范机器人和欺诈行为

保护用户以防帐户接管，阻止影响最终用户体验的恶意机器人。机器学习模型与客户端、网络和威胁情报相结合，有效阻止恶意僵尸网络、凭据和信用卡填充、内容抓取以及库存囤积行为。

管理 AI 爬虫和机器人

阻止 AI 爬虫，向其收费，或使其陷入无限循环，从而更好地控制内容和成本。全面掌握请求模式以及是否符合站点的 robots.txt 指令。所有 Cloudflare 客户均可使用。

主要功能	
检测引擎	
机器学习	我们的全球机器学习模型通过整个 Cloudflare 全球网络（每天代理数十亿个请求）的流量训练，用于识别自动流量和人类流量。此项已包含在我们的总体机器人评分中。客户会自动更新到最新模型。
异常检测	基于客户流量随时间变化的模式，我们的无监督学习行为异常模型会对应用的特定流量模式进行基线建模并校准规则阈值，以识别异常机器人行为。此项已包含在我们的总体机器人评分中。
启发式算法	我们利用以往机器人流量中已知的恶意机器人行为模式来识别机器人。我们会定期为所有客户更新启发式算法。此项已包含在我们的总体机器人评分中。
已验证机器人和 AI 机器人	我们的机器人目录会识别已知机器人检测 ID，此类机器人执行合法功能并以验证机器人身份透明运作，符合 Cloudflare 已验证机器人策略的规定。我们为已知的 AI 机器人设立了一个单独的类别，这些机器人可能遵守或不遵守 robots.txt 协议，并且可能会对您的应用隐藏其行为。
JavaScript 检测	JavaScript 检测模块在任意请求的客户端注入一段轻量级、无感知的 JavaScript 代码，以此识别无头浏览器及其他恶意指纹。我们秉持非常严格的隐私标准，在此过程中不会收集任何个人可识别信息。
机器人评分	使用机器人评分，编写更少的规则即可识别大多数机器人，而不用为每个机器人 ID 或类型编写规则。机器人评分整合来自我们检测引擎的情报，产生一个 1 到 99 的分值，指示该请求来自机器人的可能性。1 分表示肯定是自动请求，99 分表示肯定是人类请求。
通过移动设备 SDK 进行设备验证	这些 SDK 适用于所有主流移动应用平台，包括 Android、iOS、React Native、Unity 等，能够验证应用完整性，检测不安全环境，并对 API 流量进行身份验证（使用自行提供或 Cloudflare 批准的加密令牌）。
策略与响应	
标准响应	设置阻止、允许、记录、速率限制或各种用户友好的质询，对我们的检测引擎识别的机器人流量做出响应。
自定义响应策略	将 Bot Management 信号整合到其他 Cloudflare 产品（如 Cloudflare WAF 和 DDoS）的策略中，并通过 Workers 编写自定义操作。
分析	
Cloudflare 仪表板	审查最长 30 天内的机器人活动，并根据机器人评分以及其他机器人、流量和请求筛选条件进行过滤。机器人反馈循环允许客户向 Cloudflare 报告任何误报或漏报，以供进一步调查。
第三方工具（SIEM、数据湖、分析工具等）	通过 Cloudflare Security Analytics 在一个仪表板中分析您所有应用的 Bot Management 信号，在 Log Explorer 中探索更多日志数据，并通过 Log Push 在第三方 SIEM 或分析平台将第三方数据与 Cloudflare 数据进行结合。

若希望了解更多信息，欢迎注册我们的应用安全演示系列。