AKAMAI 产品简介

Content Protector

防范日渐复杂的抓取程序攻击，保护您的收入

攻击者通过抓取您的内容获利，而您却因此遭受损失。虽然公开分享内容是一种战略选择，但区分消费者参与活动与恶意抓取活动至关重要。竞争对手和攻击者可能会利用抓取到的数据，恶意破坏您的定价策略，导致您失去客户。Akamai Content Protector 具有专为抓取程序攻击定制的独特检测工具和技术，可快速识别和阻止抓取程序。因而，可在不影响速度和性能的情况下，保护您的业务和收入。

内容抓取攻击对在线业务造成了持续的困扰。与具有明确开始时间和结束时间的典型网络威胁不同，抓取程序能够持续访问您的网站。若不采取防范措施，势必会对您的业务造成严重的影响。这些影响包括：

- **网站性能影响：**持续的抓取活动会拖慢网站速度，引发用户不满，进而降低转化率。
- **处于竞争劣势：**竞争对手可能会通过内容抓取技术来监控和压低您的定价，从而影响您的收入。
- **品牌声誉风险：**仿冒者可能会滥用抓取到的内容，以您品牌的名义销售伪劣产品。

当然，抓取程序已经存在多年。但为什么现在的情况变得更糟了呢？打击抓取程序的紧迫性最近确实有所增加。2020 年的疫情和随后的供应链中断事件，使内容抓取攻击可获得更多的金钱回报。高需求商品，无论是日常必需品还是奢侈品和旅游服务，都成为了老练的内容抓取攻击活动的主要目标。

为了获得更多的潜在收益，爬虫程序操纵者开始疯狂创新，他们专注于开发各种工具，例如遥测技术，并将这些工具与其他爬虫程序操纵者的工具进行整合，从而构建出高度专业化的爬虫程序，专门用于实施内容抓取攻击。这使得抓取程序变得更为危险，且检测难度更大。更糟糕的是，内容抓取攻击还可能通过其他方法（例如插件）进行，因此仅仅依靠爬虫程序管理来遏制抓取程序是远远不够的。

但是，您不能简单地阻断所有抓取程序。例如，搜索抓取程序可找到您希望在公共搜索中展示的新内容，某些消费者购物爬虫程序可使您的产品在比价网站上更醒目，而合作伙伴也可以高效地收集最新的产品信息并与其客户分享。

对企业的好处

提高转化率
清除那些使网站和应用程序变慢的爬虫程序，留住更多客户并增加销售额

降低成本
避免为爬虫程序流量付费

阻止黄牛倒卖程序
通过防范抓取程序对您的网站进行 ping 操作，以使其无法掌握热销库存商品的抢购时间，进而大大降低爬虫程序操纵者在库存囤积攻击链中实施后续行动的能力

挫败竞争对手
防止竞争对手通过自动抓取来压低您的价格，从而保护您的销售额

抵御仿冒活动
遏制仿冒者不断抓取内容，防止他们盗取您的内容并冒充您的网站

更好地优化市场营销策略
在分析您的网站流量时，排除爬虫程序流量的干扰，以确保针对真实用户来制定优化策略

Akamai Content Protector 拥有独特的检测技术，专为检测并阻止抓取程序而设计。此外，我们还会利用 Akamai 网络的监测能力、我们在爬虫程序管理方面的全球优势，不断开发先进的检测技术。我们会根据威胁的不断演变，通过自动整合来自威胁情报研究人员和数据科学家的见解，及时更新您的保护措施，进而确保 Content Protector 在抓取程序的定制检测领域始终保持领先地位。

在抓取程序得到遏制后，您便可充分挖掘您数字资产的价值，例如提升网站性能和转化率，同时减少竞争对手的影响。

主要功能

- **检测：**一组采用机器学习的检测方法，用于评估收集到的客户端和服务器端数据。
  - » **协议级评估：**协议指纹识别技术可以评估客户端在 OSI 模型的不同层（TCP、TLS 和 HTTP）上与服务器建立连接的方式，以验证协商的参数是否符合最常见的网络浏览器和移动应用程序所期望的参数。
  - » **应用程序级评估：**评估客户端能否运行采用 JavaScript 编写的一些业务逻辑。当客户端运行 JavaScript 时，Content Protector 会收集设备和浏览器特征以及用户偏好（指纹识别）。这些不同的数据点将与协议级数据进行对比和交叉检查，以验证一致性。
  - » **用户交互分析：**行为指标可评估用户通过触摸屏、键盘和鼠标等标准外围设备与客户端进行的交互。缺少交互或出现异常交互通常与爬虫程序流量相关。
  - » **用户行为监控：**分析用户浏览网站的历程。僵尸网络通常会寻找特定内容，因此在行为上与合法流量存在显著不同。
  - » **无界面浏览器检测：**在客户端运行的自定义 JavaScript 可以发现无界面浏览器留下的迹象，即使该浏览器处于隐身模式也可被发现。
- **风险分类：**根据评估期间发现的异常，对流量进行确定性、切实可行的风险分类（低、中、高）。
- **响应操作：**一组响应策略，包括简单的监控和拒绝操作，以及更高级的操作，如 Tarpit，它能够模拟服务器停机或进行各种质询操作。在处理潜在的误报时，加密质询相较于验证码质询更加便于用户操作。

Content Protector 的基础：Akamai 生态系统

Akamai 使互联网变得快速、智能、安全。我们的综合解决方案基于全球分布式 Akamai Connected Cloud 构建，通过统一且可自定义的 Akamai Control Center 进行管理以获得可见性和控制力，并由专业服务专家提供支持，这些专家可帮助您轻松启动和运行解决方案，随着您的战略发展激发创新。

注册以获取演示或者联系 Akamai 销售团队。