阿里云
爬虫风险管理

产品简介

文档版本：20190428

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 什么是爬虫风险管理.....1
2 核心功能..... 2
3 产品优势..... 3
4 应用场景..... 4

1 什么是爬虫风险管理

云盾爬虫风险管理（Anti-Bot Service，简称Anti-Bot）是一款网络应用安全防护产品，可有效检测高级爬虫，降低爬虫、自动化工具对网站业务的影响。

云盾爬虫风险管理提供从Web、APP、到API接口一整套全面的恶意Bot防护解决方案，避免由于业务中某一环节的防护薄弱而导致的安全短板。

购买开通Anti-Bot产品后，您只需要将您的网站域名解析到Anti-Bot产品提供的CNAME地址，并在爬虫风险管理控制台中配置源站服务器IP，即可启用防护。将网站域名接入Anti-Bot产品后，您网站所有的公网流量都将先经过Anti-Bot实例，所有恶意爬虫流量都将在云端被检测、过滤，最终将正常的流量返回给源站服务器，从而确保源站业务免受恶意爬虫流量引发的数据泄露、业务欺诈等安全问题的影响。

2 核心功能

云盾防爬虫风险管理主要提供以下功能。

- 防护效果可视化：对风险及在线策略进行实时异动监控，并提供防护效果的汇总报表。
- 恶意Bot流量精准拦截：多维度刻画并过滤Bot流量，防护业务避免遭受损失。
- 云端共享威胁情报：利用云端优势共享海量的威胁情报，并对行业内集中性攻击作出快速对抗响应。
- 丰富的处置方式手段：针对可疑机器流量请求，可直接拦截，同时提供自定义UI滑块验证交互。

3 产品优势

云盾爬虫风险管理产品具有以下优势。

风险生态体系

- 通过跨多行业的爬虫行为分析，利用关系网络实现恶意爬虫的扩充发现。
- 爬虫在行业性业务目的方面非常明确，利用生态体系达成行业内协同防御。
- 沉淀网络黑灰产业中已知常用的针对性恶意爬虫的IP/User Agent数据。
- 共享亿级由阿里巴巴集团业务经验沉淀的风险情报。

云端部署

- 部署在恶意Bot流量到达源站前，通过识别、过滤，使您的业务源站避免遭受攻击压力。
- 云上资源支持弹性扩容，针对业务高峰可自由收缩，具备百万级QPS业务的风险防控能力。
- 由专业安全技术团队提供产品策略的持续更新，快速下发最新的攻防规则。
- 云上可共享实时发现的恶意Bot特征，形成协同防御体系。

多层防护策略

- 提供最合适Web、H5、APP、API业务的恶意Bot防护方案。
- 提供多维度的防护策略，更精准地刻画恶意Bot特征。
- 针对不同风险等级的恶意Bot，提供不同的处置手段。

4 应用场景

云盾爬虫风险管理在以下场景中都能为您的业务提供安全防护，有效避免业务遭受损失。

航空公司占座

黄牛党利用恶意爬虫遍历航空公司的低价票，同时批量发起机器请求进行占座，导致航班座位资源被持续占用产生浪费，最终引发航班空座率高对航空公司造成业务损失，并且损害正常用户的利益。

电商活动黄牛

黄牛党在电商活动时针对有限的高价值商品的限时秒杀、优惠活动等可牟利场景，批量发起机器请求来模拟正常的交易，再将商品、资源进行倒卖从中赚取差价，导致电商企业的营销资源无法触达正常用户，而被黄牛牟取暴利。

核心接口被刷

登录、注册、短信等业务环节作为业务中的关键节点，相关接口往往会被黑客利用，为后续的欺诈行为作准备。