天御业务安全防护

活动防刷

产品文档

腾讯云

文档目录

活动防刷
活动防刷产品简介

最近更新时间：2019-07-20 19:08:18

1. 天御活动防刷是什么

近年来电商、O2O 等行业用高额补贴、优惠等方式获取用户，同时也催生了“羊毛党”。“羊毛党”有选择性地参加线上活动，以零或者相对较低的成本获取物质优惠，严重破坏了活动目的、侵占了活动资源，使企业获取用户的成本提升、口碑和形象受损。因此，天御推出针对“羊毛党”的活动防刷服务，有效地识别出“羊毛党”，保障企业利益。

2. 天御活动防刷的优势

2.1 完善的服务体系

快速部署服务体系，前期专业的恶意诊断，提供最优安全策略，后期重大活动专人跟进，全面分析实时数据报表。

2.2 腾讯同款安全服务

天御防刷服务已为腾讯多款产品和业务提供完善的帐号保护体系，经历了数亿用户十年的考验。

活动防刷购买指南

最近更新时间：2018-12-17 10:42:58

腾讯云活动防刷 AA 提供按次调用的包年套餐，适合有大型活动或长期请求量较大的安全活动需求场景。

定价详情：

次数	价格（元/年）
50万	5万
100万	8万
300万	12万
1000万	20万
30000万	150万
90000万	360万
200000万	600万

若在次数包还未用完时再次购买，则按照次数包叠加计费规则计算。

说明：

叠加计费规则为

- 可使用次数为新购次数包+原剩余未使用次数。
- 有效时间从新购次数包开始计算，一年内有效。

次数包用完后，超出次数会按照后付费价格区间表月结。

说明：

付费价格区间表：

次数区间	次/元
50万以内	0.100
50万以上-300万以内	0.040
300万以上-1000万以内	0.020

1000万以上-3000万以内	0.010
3000万以上-10000万以内	0.006
10000万以上	0.006

活动防刷开发指引

最近更新时间：2019-08-01 17:49:01

开发者需要通过调用云 API 的天御相关接口完成接入，接入 API 步骤如下：

1. 获取腾讯云密钥

如果您已经具有了腾讯云密钥则可以跳过这一步。进入云 API 密钥，在左侧导航栏中单击【API 密钥】，进入 API 密钥页面，单击【新建密钥】。

2. 进入天御业务安全防护管理中心

进入管理中心>云产品>天御业务安全防护。

3. 申请权限

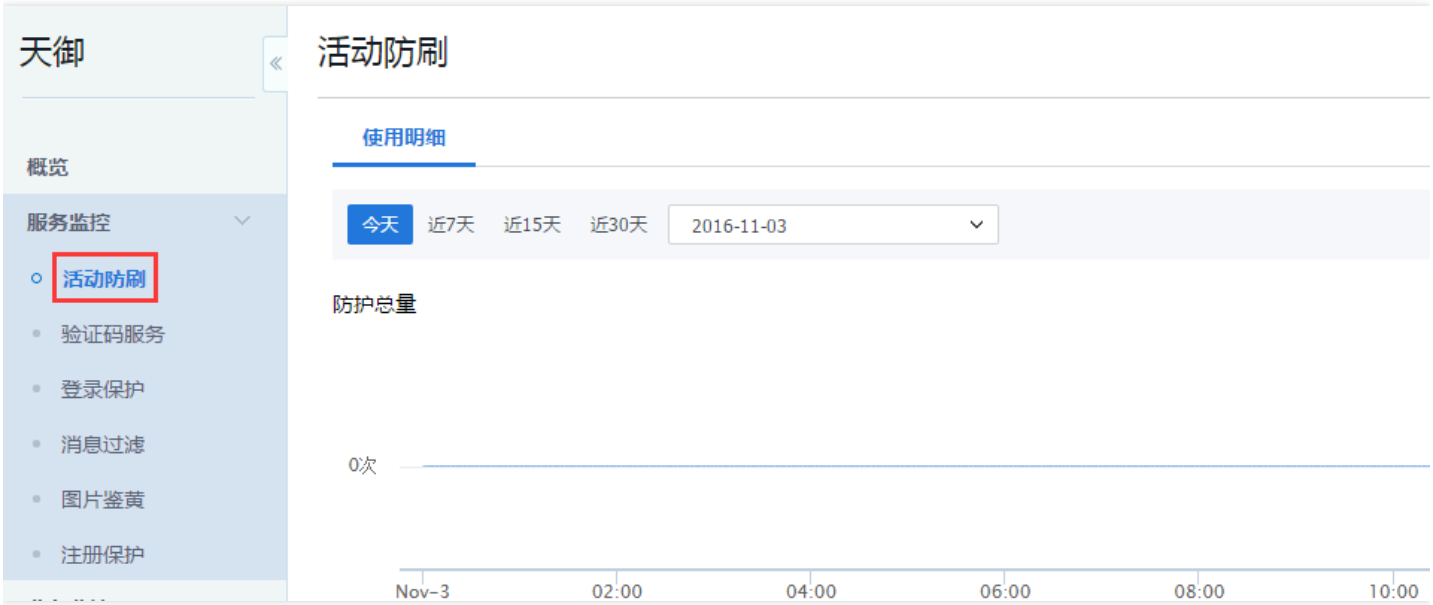
在天御业务安全防护管理中心中单击"活动防刷服务"免费体验，确定开通。

4. 按照指定API写代码

活动防刷API

5. 查询调用数据

进入天御业务安全防护管理中心，单击【服务监控】，即可查询到对应服务的调用数据。



活动防刷 API 文档

最近更新时间：2019-09-19 09:12:55

接口描述

协议：HTTPS Post
域名： csec.api.qcloud.com
接口名：ActivityAntiRush

输入参数

注意：
以下所有参数在入参时，请正确传参，不能传入空值。

参数	是否必选	参数类型	参数描述
accountType	是	Uint	用户账号类型（QQ 开放帐号、微信开放账号需要 提交工单 由腾讯云进行资格审核）： • 1：QQ 开放帐号。 • 2：微信开放账号。 • 4：手机号。 • 0：其他。 • 10004：手机号 MD5。
uid	是	String	用户 ID 不同的 accountType 对应不同的用户 ID。如果是 QQ，则填入对应的 openid，微信用户则填入对应的 openid/unionid，手机号则填入对应真实用户手机号（如13123456789）。
userIp	是	String	用户领取奖励时的真实外网 IP。
postTime	是	Uint	用户操作时间戳，单位秒（格林威治时间精确到秒，如1501590972）。
appId	否	String	accountType 是QQ或微信开放账号时，该参数必填，表示 QQ 或微信分配给网站或应用的 AppID，用来唯一标识网站或应用。

参数	是否必选	参数类型	参数描述
nickName	否	String	昵称，UTF-8 编码。
phoneNumber	否	String	手机号。若 accountType 选4（手机号）、或10004（手机号 MD5），则无需重复填写。否则填入对应的手机号（如15912345687）。
emailAddress	否	String	用户邮箱地址（非系统自动生成）。
registerTime	否	Uint	注册时间戳，单位：秒。
registerIp	否	String	注册来源的外网 IP。
cookieHash	否	String	用户 HTTP 请求中的 cookie 进行2次 hash 的值，只要保证相同 cookie 的 hash 值一致即可。
address	否	String	地址。
loginSource	否	UInt	登录来源： • 0：其他。 • 1：PC 网页。 • 2：移动页面。 • 3：App。 • 4：微信公众号。
loginType	否	UInt	登录方式： • 0：其他。 • 1：手动账号密码输入。 • 2：动态短信密码登录。 • 3：二维码扫描登录。
loginSpend	否	Uint	登录耗时，单位：秒。
rootId	否	String	用户操作的目的 ID，如点赞等，该字段就是被点赞的消息 ID，如果是投票，则为被投号码的 ID。
referer	否	String	用户 HTTP 请求的 referer 值。
jumpUrl	否	String	登录成功后跳转页面。
userAgent	否	String	用户 HTTP 请求的 userAgent。
xForwardedFor	否	String	用户 HTTP 请求中的 x_forward_for。
mouseClickCount	否	Uint	用户操作过程中鼠标单击次数。
keyboardClickCount	否	Uint	用户操作过程中键盘单击次数。

参数	是否必选	参数类型	参数描述
macAddress	否	String	MAC 地址或设备唯一标识。
vendorId	否	String	手机制造商 ID，如果手机注册，请带上此信息。
imei	否	String	手机设备号。
appVersion	否	String	App 客户端版本。
businessId	否	Uint	业务 ID 网站或应用在多个业务中使用此服务，通过此 ID 区分统计数据。
wxSubType	否	int	• 1：微信公众号。 • 2：微信小程序。
randNum	否	String	Token 签名随机数，微信小程序必填，建议16个字符。
wxToken	否	String	• 如果是微信小程序，该字段为以 ssesion_key 为 key 去签名随机数 randNum 得到的值（hmac_sha256 签名算法）。 • 如果是微信公众号或第三方登录，则为授权的 access_token（注意：不是普通 access_token，具体看微信官方文档）。
checkDevice	否	Int	是否识别设备异常： • 0：不识别。 • 1：识别。

输出参数

参数	类型	描述
code	Int	调用接口返回码，0为正常调用。
codeDesc	String	业务侧错误码，成功时返回 Success，错误时返回具体业务错误原因。
message	String	UTF-8 编码，出错消息。
Nonce	UInt	随机正整数，与 Timestamp 联合起来，用于防止重放攻击（公共参数）。
associateAccount	String	accountType 是 QQ 或微信开放账号时，用于标识 QQ 或微信用户登录后关联业务自身的账号 ID。
postTime	String	操作时间戳，单位：秒。

参数	类型	描述
uid	String	用户 ID 不同的 accountType 对应不同的用户 ID。如果是 QQ，则填入对应的 openid，微信用户则填入对应的 openid/unionid，手机号则填入对应真实用户手机号（如13123456789）。
rootId	String	用户操作的目的 ID，如点赞等，该字段就是被点赞的消息 ID，如果是投票，就是被投号码的 ID。
userIp	String	用户操作的真实外网 IP。
level	Int	• 0：表示无恶意。 • 1 - 4：恶意等级由低到高。
riskType	Array	风险类型，详情请参见下文 **riskType 详细说明**。

riskType 详细说明：

风险类型	风险详情	风险码	说明
账号风险	账号信用低	1	账号近期存在因恶意被处罚历史，网络低活跃，被举报等因素。
	垃圾账号	2	疑似批量注册小号，近期存在严重违规或大量举报。
	无效账号	3	送检账号参数无法成功解析，请检查微信 OpenID 是否有误 。
	黑名单	4	该账号在业务侧有过拉黑记录。
	白名单	5	业务自行有添加过白名单记录。
行为风险	批量操作	101	存在 IP/设备/环境等因素的聚集性异常。
	自动机	102	疑似自动机批量请求。
	微信登录态无效	104	检查 wxtoken 参数，是否已经失效。
环境风险	环境异常	201	操作 IP/设备/环境存在异常。当前 IP 为非常用 IP 或恶意 IP 段。
	JS 上报异常	202	需要用户在前端部署 JS 方有效。
	撞库	203	该账号有过“撞库”的历史行为。
	非公网有效 IP	205	传进来的 IP 地址为内网 IP 地址或者 IP 保留地址 。
	设备异常	206	该设备存在异常的使用行为。

示例代码

一个完整的请求需要两类请求参数：公共请求参数和接口请求参数。本文只列出了接口请求参数，并未列出公共请求参数，有关公共请求参数的更多说明，请参见 公共请求参数。公共参数传参中不需要添加 SignatureMethod 参数，签名计算默认使用 HmacSHA1 的签名算法，示例代码中有具体实现。

- **请求示例**

```
<https://csec.api.qcloud.com/v2/index.php?Action=ActivityAntiRush
&<公共请求参数>
&secretId=AKIDmQtAxYTAB2iBS8s2DCzazCD2g7OUq4Zw
&accountType=1
&uid=D692D87319F2098C3877C3904B304706
&userIp=127.0.0.1（调用时必须是外网有效 IP 地址）
&postTime=1553484280（uinx 时间戳，仅需要精确到秒）
```

- **响应示例**

```
{
"Nonce": 516529719,
"code": 0,
"level ": 1,
"message": "NoError",
"postTime": "1553484280",
"uid": "D692D87319F2098C3877C3904B304706",
"userIp": "127.0.0.1",
"riskType": [1]
}
```

- **代码下载**
  - Python 示例
  - PHP 示例
  - Java 示例
  - .Net 示例

天御打击羊毛党方案

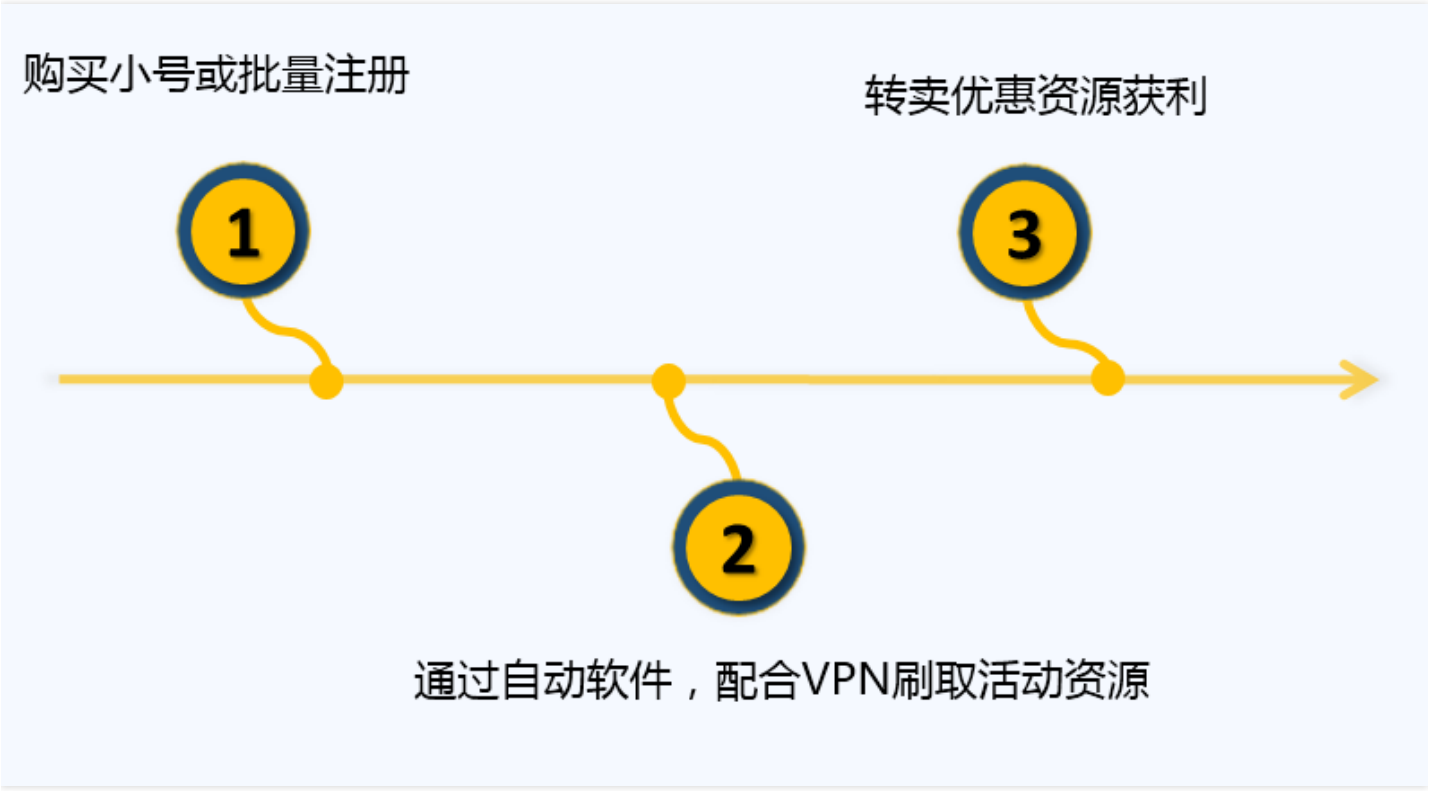
最近更新时间：2019-08-09 17:35:18

1. 背景介绍

最近1 - 2年电商行业飞速发展，各路人马包括大量的创业公司都在 O2O 这一领域深挖、布局，都想抢占这个一个万亿级的市场先机，商家不惜通过各种活动形式的高额补贴来获取用户、培养用户的消费习惯。整个行业的补贴可以说是放血式的，一张优惠券少则几块多则几十块，尤其是P2P理财更高达上百块，根据之前一家权威媒体的估计，打车行业因为补贴亏损高达29亿，团购行业28亿，都处于大幅度投入期。但是，高额的补贴、优惠在获取用户的同时了也催生了“羊毛党”。“羊毛党”有选择性的参加线上的活动，从而以相对较低或者零成本获取物质上的优惠，他们的行为距离欺诈只有一步之遥，他们严重破坏了活动的目的、侵占了活动的资源，使得企业获取用户的成本在提升、损坏企业口碑和形象；因此，针对“羊毛党”的打击势在必行。

2. 羊毛党现状

“羊毛党”一般先利用自动机注册大量的目标网站的账号，当目标网站搞促销、优惠等活动的时候，利用这些账号参与活动刷取较多的优惠，最后通过各类平台转卖获益，“羊毛党”获利基本过程如图所示：



3. 天御对抗思路

一般的活动，都会限制一个账号的参与次数，要想获取高额的收益，“羊毛党”就必须掌握大量的虚假账号。因此，对抗的本质就是识别虚假账号，一般来
讲主要从三个环节入手：

3.1 注册环节

识别虚假注册、减少“羊毛党”能够使用的账号量。在注册环节识别虚假注册的账号，并进行拦截和打击。

3.2 登录场景

提高虚假账号登录门槛，从而减少能够到达活动环节的虚假账号量。例如，登录环节通过验证码、短信验证码等手段来降低自动机的登录效率，从而达到
减少虚假账号登录量，减轻活动现场安全压力的目的。

3.3 活动环节

这个是防刷单对抗的主战场，也是减少“羊毛党”获利的直接战场；这里的对抗措施，一般有两个方面：

3.3.1 通过验证码（短信、语音）降低黑产刷单的效率。

3.3.2 大幅度降低异常账号的优惠力度。

4. 天御解决方案

针对注册、登录和活动环节，天御提供了对应的接口用于保障业务系统的安全。