反欺诈

产品简介

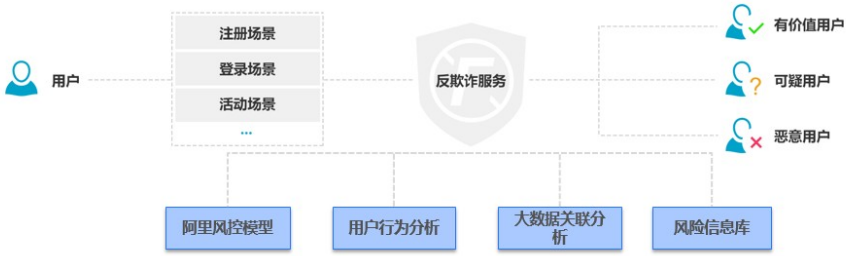
阿里云
aliyun.com

产品简介

反欺诈服务产品概述

简要介绍

反欺诈服务是基于阿里大数据风控服务能力，通过领先的行为收集技术和机器学习模型，解决企业账号、活动、支付等关键业务环节存在的欺诈威胁。



功能描述

风险识别服务

通过用户行为信息、软硬件环境信息、设备指纹等综合判定用户请求的风险程度：可信、可疑、风险，业务根据风险结果进行相应处理：直接进入业务流程，图形/短信/邮箱验证，直接拦截，离线分析等。
客户平台集成风险识别服务方式：前端引入JS脚本获得风险请求唯一ID，服务端根据风险请求唯一ID调用风险识别API，获得本次请求风险识别结果。

风险拦截服务

通过引入前端拦截组件对用户请求进行验证，可信用户通过验证直接进入业务流程，恶意用户拦截。

客户平台集成风险拦截服务方式：前端引入组件JS获得滑动通过签名串，服务端调用风险拦截API验证签名串，获得签名串验证结果。

风险用户查询服务

通过用户基础信息(IP\手机\邮箱等)判断用户风险程度：可信、可疑、风险，业务根据风险结果进行相应处理：直接进入业务流程，图形/短信/邮箱验证，直接拦截，离线分析等。
客户平台集成风险用户查询服务方式：服务端调用风险用户查询API，传入IP、手机、邮箱等用户基础信息，获得用户风险结果。

风险防控

防垃圾注册

注册是恶意账号产生的源头，反欺诈服务能识别和打击网络上的"羊毛党"通过注册机和虚假手机号码、人工打码等方式批量注册的账号，从而降低平台在登陆、活动等场景的风险和压力。

防营销作弊

平台推广活动时，"羊毛党"、"刷单客"会通过批量注册、购买小号、，批量套取优惠，给平台造成不必要的资金损失。反欺诈服务实时识别活动推广过程中的作弊行为，让真正有价值的客户享受到活动奖励，提升营销效果。

防恶意登陆

登陆网络的欺诈分子会通过机器对账户密码进行暴力破解，或利用互联网中大量泄露的用户名密码进行尝试，进一步获得账户登录权限。反欺诈服务实时对登陆环节可能存在的风险进行检测和防控，从而有效防止用户信息泄露。

支付保护

登陆网络的欺诈分子通过木马钓鱼等方式获得用户支付账号信息并进行支付行为。反欺诈服务实时检测交易支付、转账、提现等支付环节存在的异常情况，防止盗卡支付风险。

反垃圾服务

登陆网络的欺诈分子利用互联网恶意群发大量的非法广告、黄色图片、违禁内容等，严重影响用户上网体验，阻碍网络健康发展。反欺诈服务通过大数据分析，实时自动过滤灌水贴、违规信息、站内垃圾消息等，从而提升整个网站UGC质量。

产品结构

反欺诈服务名词解释

各类型欺诈威胁

垃圾注册

平台推广拉新客户活动时，常常吸引网络上的"羊毛党"通过注册机和虚假手机号码、人工打码等方式批量注册一批账号，进入平台批量套取优惠。

暴力破解

登陆网络的欺诈分子会通过机器对账户密码进行暴力破解，进一步获得账户登录权限，从而导致用户信息泄露及资金受损

撞库

登陆网络的欺诈分子利用互联网中大量泄露的用户名密码进行尝试，如果账户、密码不幸在泄露库中，可能导

致关联平台上的账号被不法分子盗用

营销作弊

平台推广活动时，欺诈分子会通过模拟器、虚假手机号码、人工打码等方式绕过平台验证，批量套取优惠，给平台造成不必要的资金损失

盗卡支付

登陆网络的欺诈分子通过木马钓鱼等方式获得用户支付账号信息并进行支付行为，导致用户资金损失，影响企业品牌形象

垃圾内容

登陆网络的欺诈分子利用互联网恶意群发大量的非法广告、黄色图片、违禁内容等，严重影响用户上网体验，阻碍社交网络的健康发展

反欺诈服务产品优势

精准的风险识别率

依据历史大数据分析，风险识别准确率高于95%。

业内领先的验证技术

通过创新的验证技术，极大提高对恶意用户的拦截能力。

多平台的防控

同时支持WEB和移动平台的风险防控

稳定可靠的系统支持

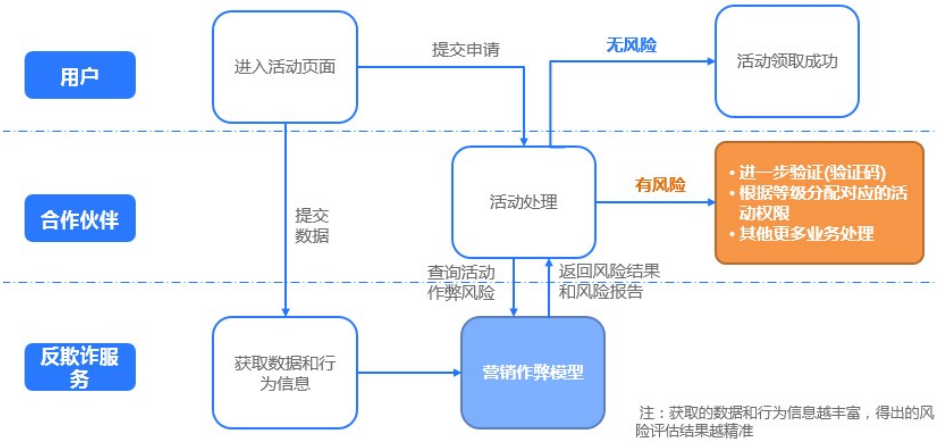
高于99.99%的可用性、毫秒级响应时间、每秒万级并发量，保障业务顺利进行

反欺诈服务使用场景

使用场景

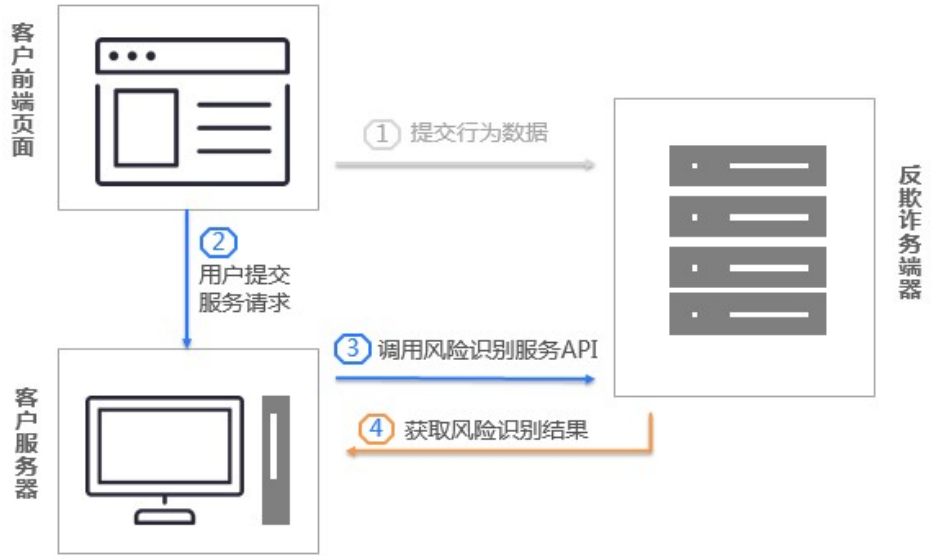
注册、登陆、活动、支付、交易评价、论坛 、微博

以活动为例



反欺诈服务基础架构

风险识别服务



1.提交行为数据

a) 此步骤会由前端引入的JS自助完成，无需客户平台处理。

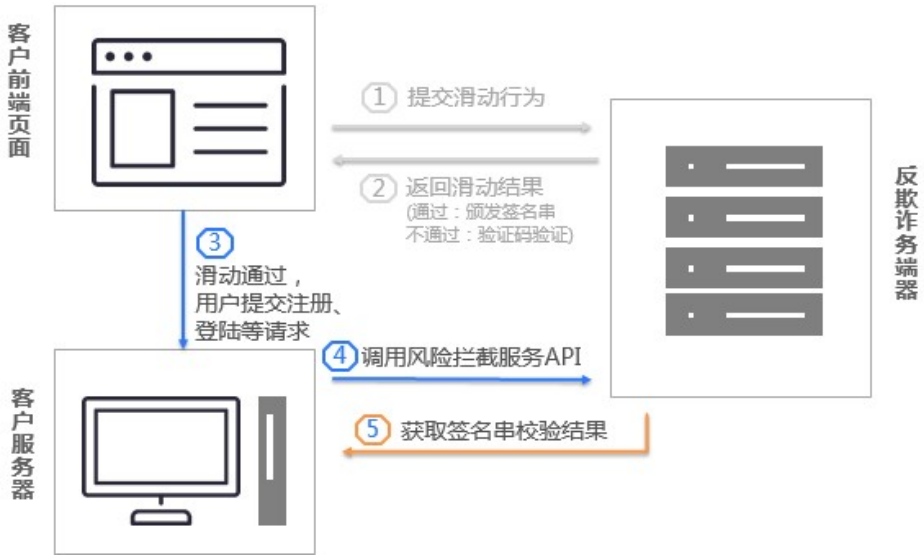
b) 提交的行为数据包括：

- 浏览器名称、版本
- 操作系统
- 屏幕长宽
- 鼠标点击、移动
- 键盘敲击
- 屏幕滑动轨迹
- URL
- 是否安装Flash

2.调用风险识别服务API
由客户服务端调用风险识别服务API，获取风险评估结果。风险评估结果，可做为其中一个因子参与到业务决策逻辑中，也可根据评估结果直接进行处置，如：

- 可信，直接进入业务流程，对用户无感知；
- 可疑，进一步验证、或打标记观察；
- 风险，直接拦截，或将业务权限级别调低。

风险拦截服务



1.提交滑动行为
a) 此步骤会由前端引入的JS自助完成，无需客户平台处理。
b) 提交的行为数据包括：

- 浏览器名称、版本
- 操作系统
- 屏幕长宽
- 鼠标点击、移动
- 键盘敲击
- 屏幕滑动轨迹
- URL

- 是否安装Flash

2.返回滑动结果

此步骤会由前端引入的JS/SDK自助完成，无需客户平台处理。

a) 可信用户：滑动直接通过，反欺诈服务端颁发签名串；

b) 可疑用户：滑动后出验证码，通过验证码校验后，反欺诈服务端颁发签名串；

c) 风险用户：滑动后拦截。

3.调用风险拦截服务API

由客户服务端调用风险拦截服务API，校验签名串。

a) 校验成功：直接进入业务流程；

b) 校验失败：返回前端进行滑动。

风险用户查询服务

1.调用风险用户查询服务API

由客户服务端调用风险用户查询服务API，传入用户基本信息，获得用户风险结果。

a）传入的用户基本信息包括：

- IP
- 手机
- 邮箱
- 账号

b）风险结果可做为其中一个因子参与到业务决策逻辑中，也可根据评估结果直接进行处置，如：

- 可信，直接进入业务流程，对用户无感知；
- 可疑，进一步验证、或打标记观察；
- 风险，直接拦截，或将业务权限级别调低。