

数据风控

产品简介

产品简介

什么是数据风控

简要介绍

数据风控由阿里聚安全提供，凝聚了阿里多年业务风控经验，专业、实时对抗垃圾注册、刷库撞库、活动作弊、论坛灌水等严重威胁互联网业务安全的风险，同时保证正常用户体验顺畅无影响。



功能描述

数据风控包含业务风控和人机验证两类功能：

业务风控

业务风控，包含：注册防控、登陆防控、活动防控、消息防控和其他风险防控，通过用户行为、软硬件环境信息、设备指纹、业务基础信息综合判定用户请求的风险程度：

注册防控：在注册场景提供安全防护，防止机器注册、人工恶意注册、注册短信被攻击。

登陆防控：在登陆场景提供安全防护，防止刷库撞库、暴力破解、可疑登陆。

活动防控：在活动场景提供安全防护，防止刷红包、抢优惠券、黄牛抢号、黄牛刷单。

消息防控：在发帖、评论场景提供安全防护，防止批量发帖、垃圾评论。

其他风险防控：其他场景下的风险防控，防止如频繁查机票、机器点赞、批量送礼物、虚假投票等。

人机验证

人机验证产品，凝聚了阿里多年人机对抗的技术沉淀，现在大量如垃圾注册、刷库撞库、薅羊毛等严重影响企

业正常业务运作的恶意风险背后，都离不开机器自动化脚本，人机验证产品在保证用户极致体验的同时，对机器风险进行有效拦截，提供给用户安全可靠的业务环境

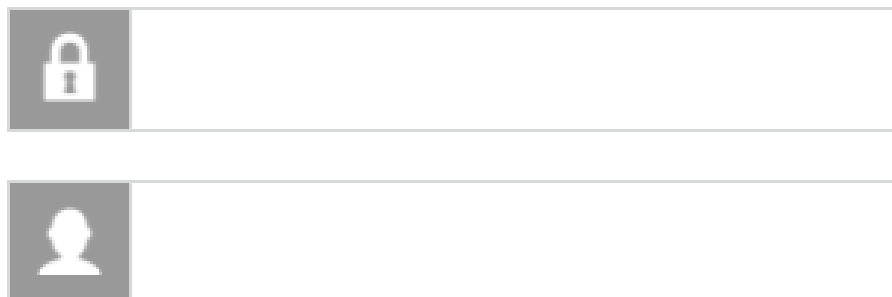
人机验证服务目前提供了滑动验证，刮刮卡，无痕验证，智能验证，投篮验证等多种验证方式，通过生物特征判定操作计算机的是人还是机器，从而取代传统验证方式。各应用展现形式如下：

滑动验证：



滑动验证界面示例：显示会员名输入框（13967143405）和验证按钮（>> 拖动滑块验证>>），下方有确定按钮。

刮刮卡：



刮刮卡界面示例：显示两个刮刮卡区域，上方区域带有锁图标，下方区域带有用户头像图标。

请摁住鼠标左键，刮出两面盾牌



登 录

智能验证：







点击按钮开始智能验证

登 录

无痕验证：





登 录

Android/iOS：

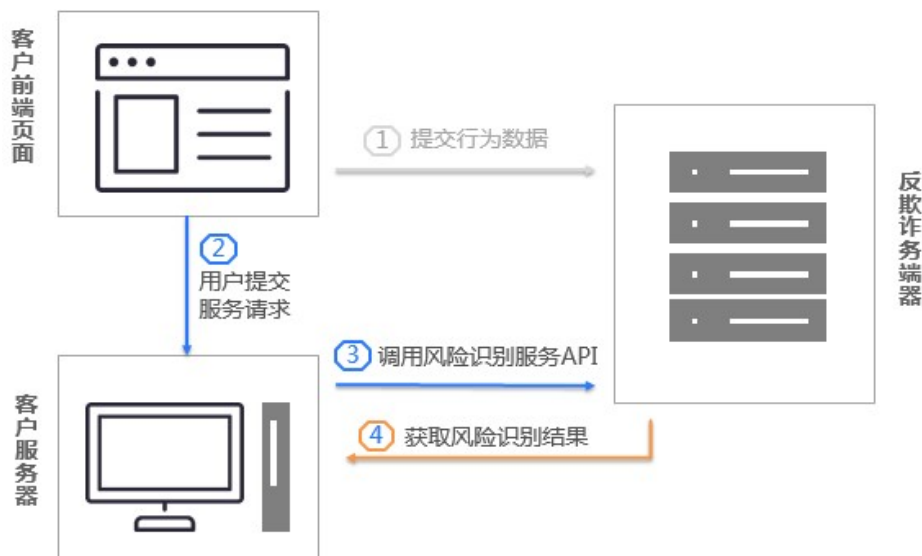


产品架构

业务风控

业务风控，包含：注册防控、登陆防控、活动防控、消息防控和其他风险防控，通过用户行为、软硬件环境信息、设备指纹、业务基础信息综合判定用户请求的风险程度。

业务风控系统间交互流程如下：



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.调用业务风控各服务API

由客户服务端调用业务风控各服务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：

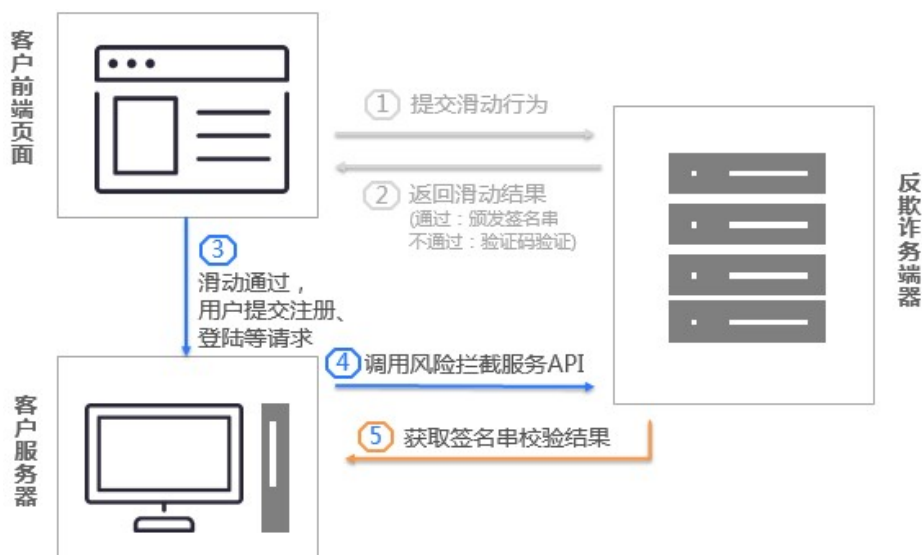
- 可信，直接进入业务流程，对用户无感知；
- 可疑，进一步验证、或打标记观察；
- 风险，直接拦截，或将业务权限级别调低。

验证码

验证码服务目前提供了滑动验证，刮刮卡，无痕验证，智能验证，通过生物特征判定操作计算机的是人还是机器，从而取代传统验证方式。

滑动验证码

滑动验证系统间交互流程如下：



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.调用验证码服务API

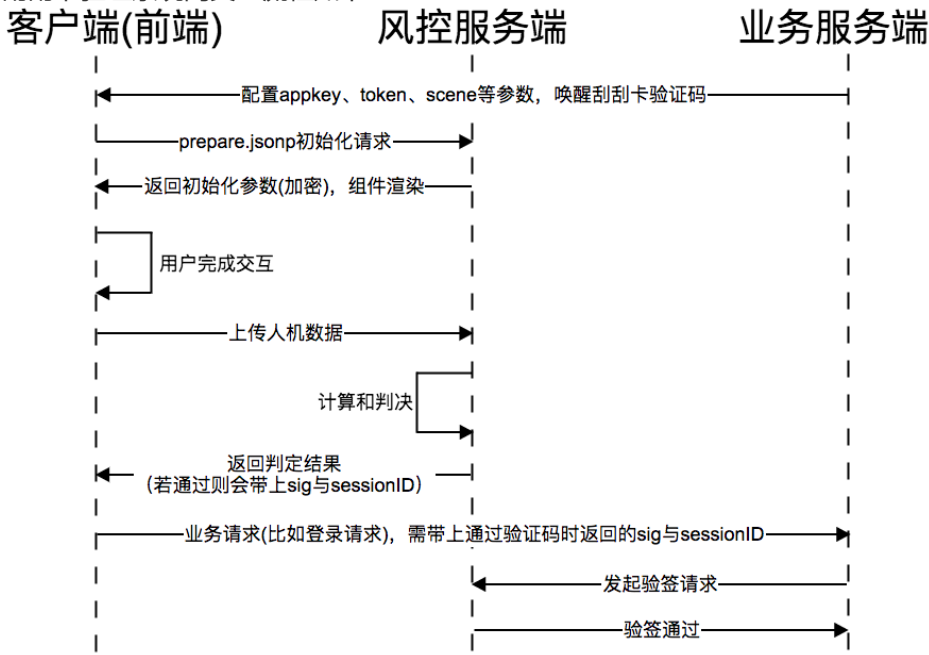
由客户服务器调用风险拦截服务API，校验签名串。

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。

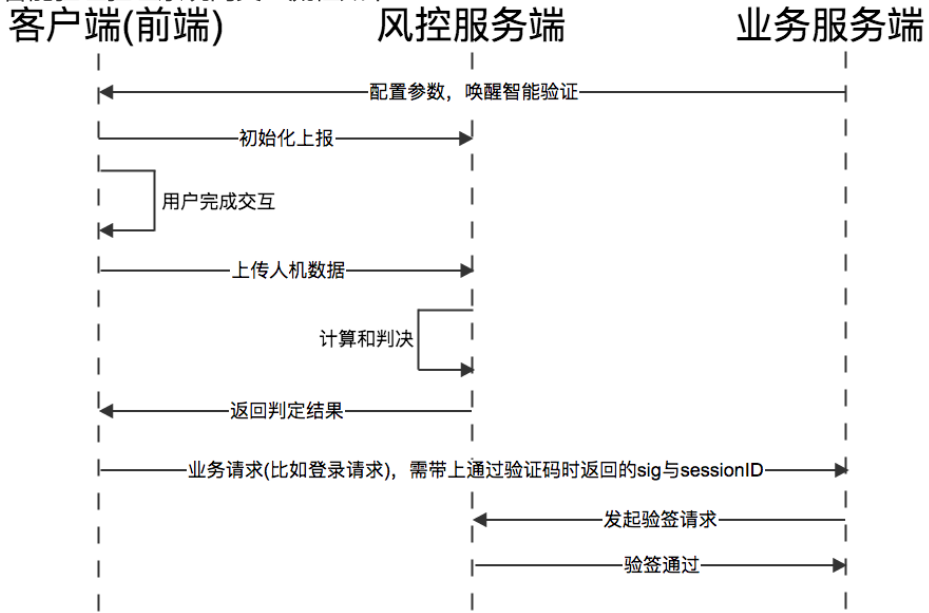
刮刮卡

刮刮卡验证系统间交互流程如下：



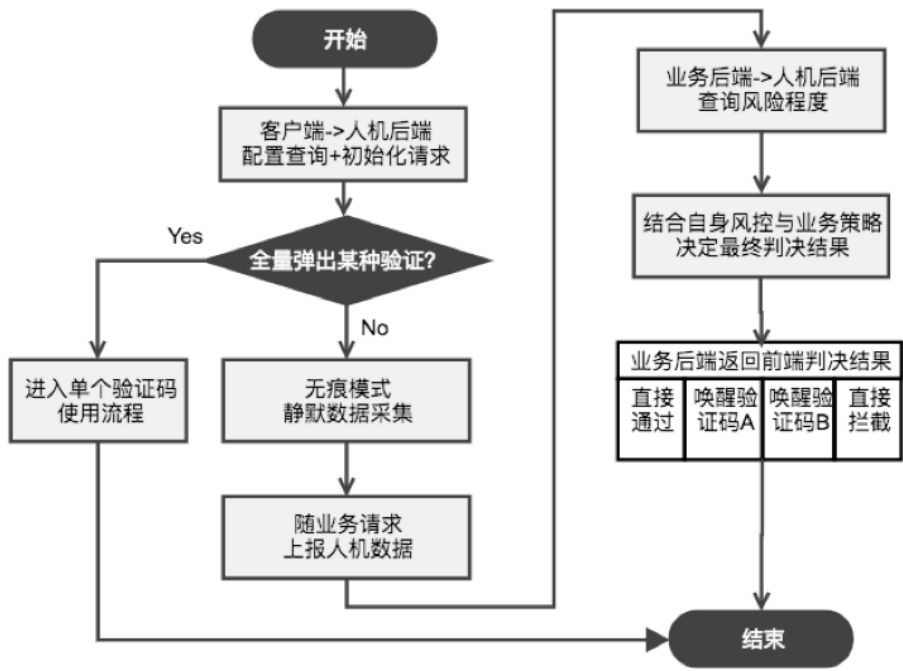
智能验证

智能验证验证系统间交互流程如下：



无痕验证

无痕验证系统间交互流程如下：



产品优势

数据风控产品优势

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

业内领先的代码保护能力

前端代码的混淆能力业内首屈一指，铜墙铁壁式的验证产品

验证产品形式丰富

根据不同的使用场景，给予丰富的人机验证产品，真正平衡安全与用户体验

极致用户体验

产品形态丰富，便捷，趣味，从各处给予用户极致的交互体验

风险二次验证

对正常请求，一次通过。对识别恶意请求，拒绝通过。对高风险请求，进行二次再验证。

高度自定义的灵活配置

用户可自定义人机验证产品各类样式，迎合业务场景需求，快速接入，高效部署

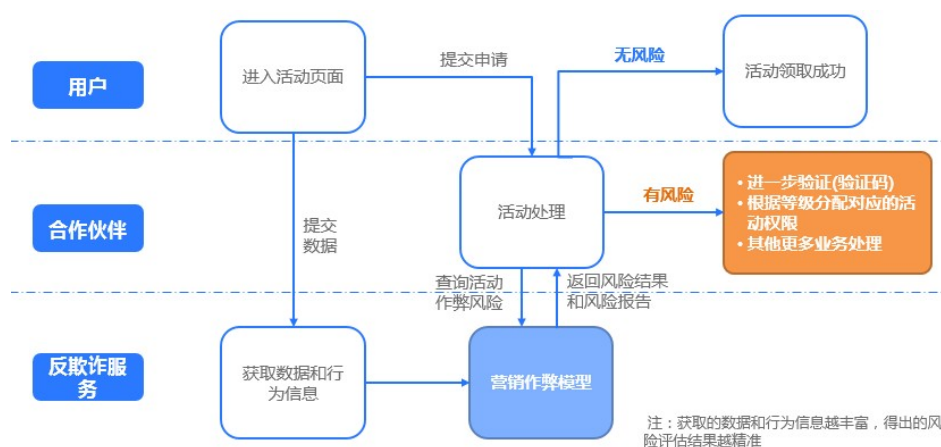
应用场景

数据风控使用场景

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



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