设备安全

产品简介

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

产品简介

产品概述

最近更新时间：2022-09-23 17:02:21

什么是设备安全产品

设备安全（TencentDevice Safety）以可信设备标识为基础，结合 AI 无感混合专家模型算法，与实际场景相结合，提供用户设备风险识别，赋能各行业安全。

产品功能

输出可信设备标识

基于 SDK 采集的设备信息，通过机器学习算法，为 Android/iOS/H5/小程序生成可信设备标识。

输出基于设备信息的风险标签

通过用户行为数据的采集和分析，实现人机识别，并结合采集信息，对可信设备标识生成设备、环境、行为等相关的风险标签和风险评分，供反欺诈规则模型使用。

版权所有：腾讯云计算（北京）有限责任公司

产品优势

最近更新时间：2022-09-23 17:02:21

可信设备标识

基于动静态特征与人工智能模型生成的高准确性、高兼容性、有效对抗设备信息篡改的可信设备标识。

设备风险识别

设备实时风险检测服务接受百亿级检测请求，在不断攻防对抗中积累下来的风险识别对抗经验，全方位有效检出各场景下的设备风险行为。

风控模型算法

经过10余年安全团队的积累，形成独特的设备风控算法及模型，可将设备风险标签应用于各种风控场景进行黑产打击。

安全体系保障

基于终端运行环境不可信原则，设计设备安全风险防控保障体系。

全链路安全防护

采用端管云全链路加密签名校验，自研协议防护数据链路安全传输，加强风险识别能力，有效对抗重放、篡改、劫持等类型风险攻击。

设备威胁态势感知

结合可信设备风控体系，采用度量学习加无监督聚类的算法，针对设备层面未知的安全风险威胁进行预测感知，有效规避潜在可能的安全风险问题。

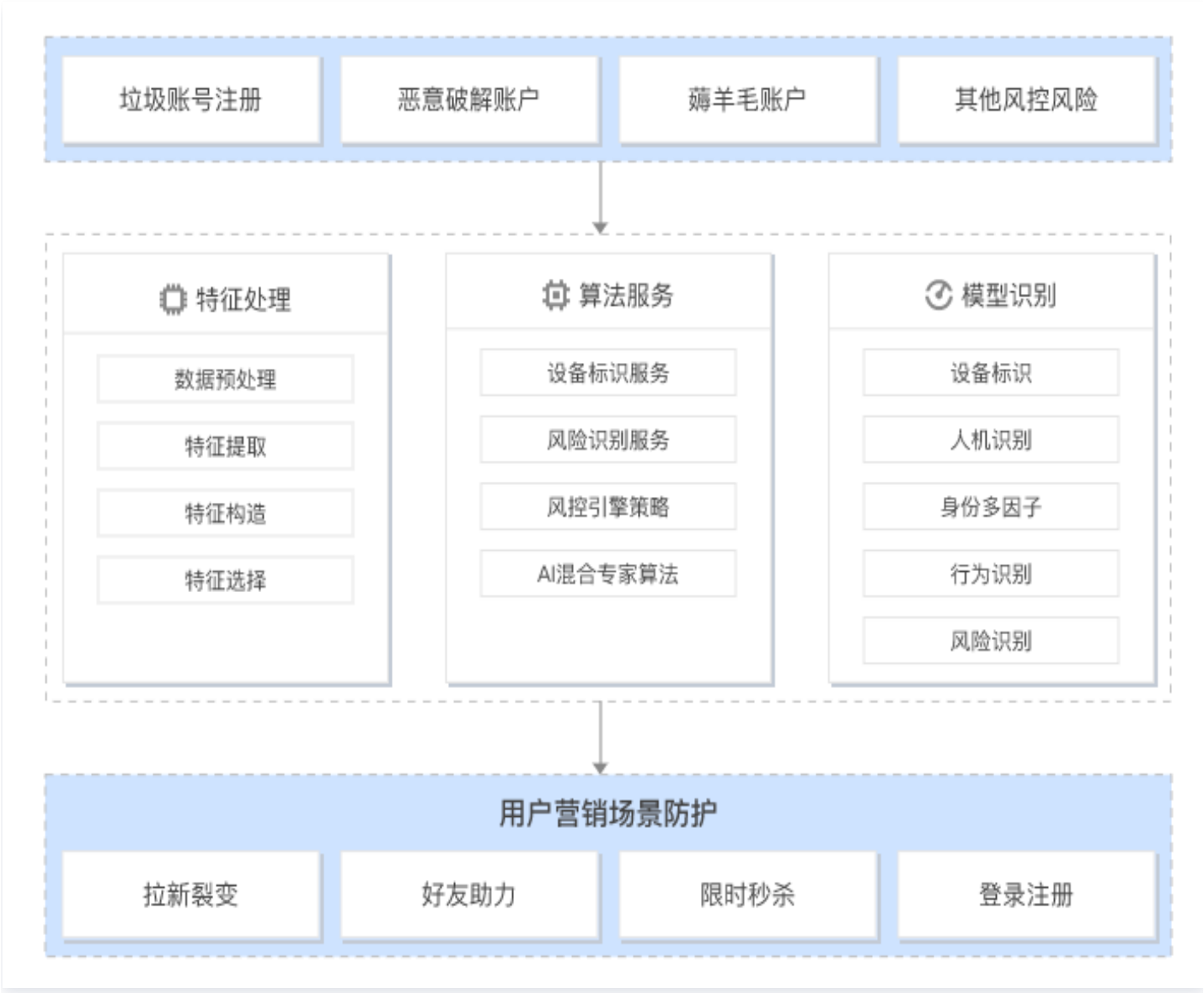
版权所有：腾讯云计算（北京）有限责任公司

应用场景

最近更新时间：2022-09-28 14:14:02

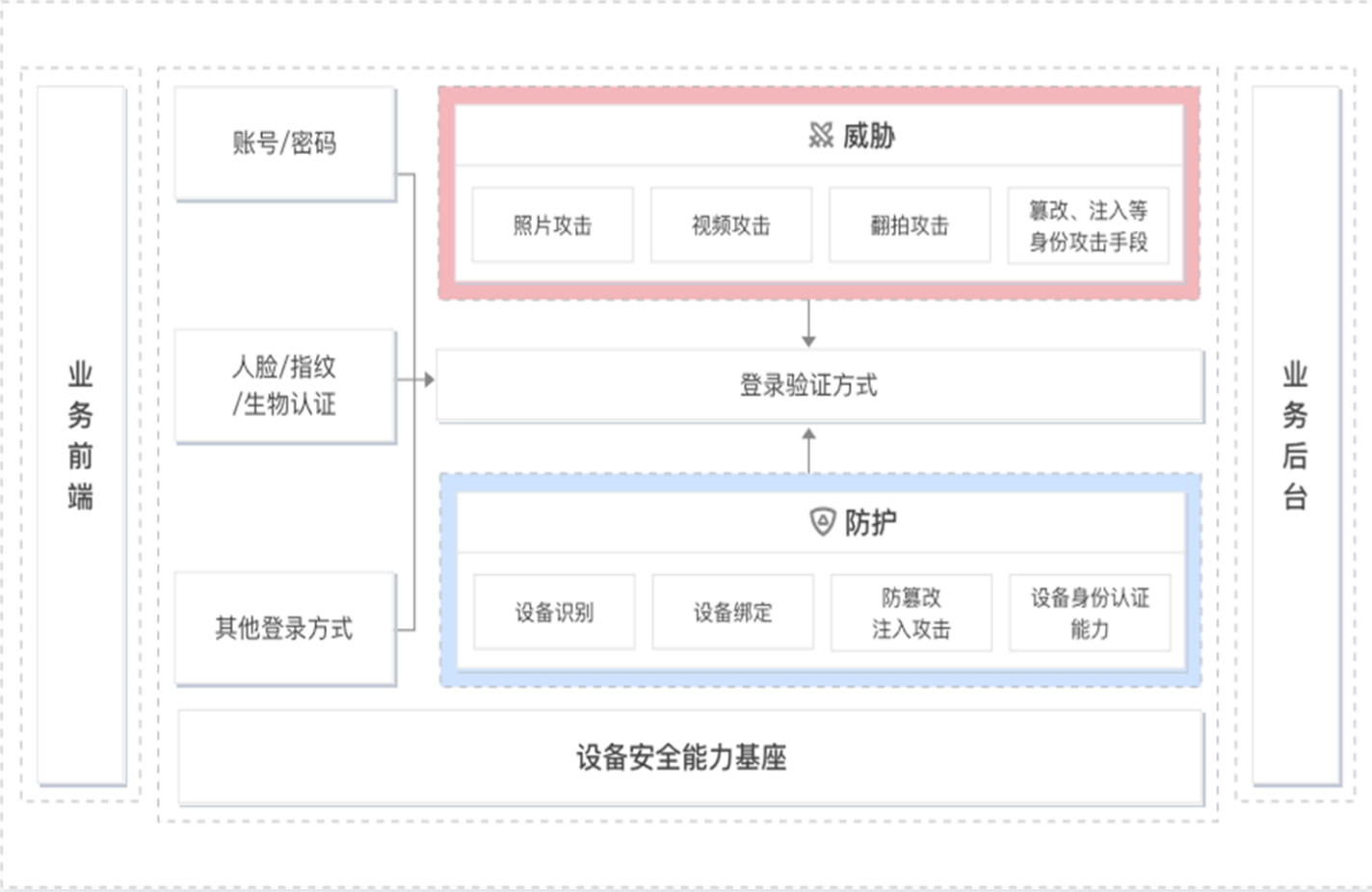
营销活动反作弊

营销活动涉及多种业务流程，在注册、登录、选购、营销业务场景中有较多的安全风险，基于设备安全方案，可精准防御模拟器、设备篡改以及群控设备风险，再通过账号、设备、IP 环境建立关联网络，利用社群发现、风险聚类算法精准防御批量、规模性欺诈活动的黑产团伙。



身份多因子认证

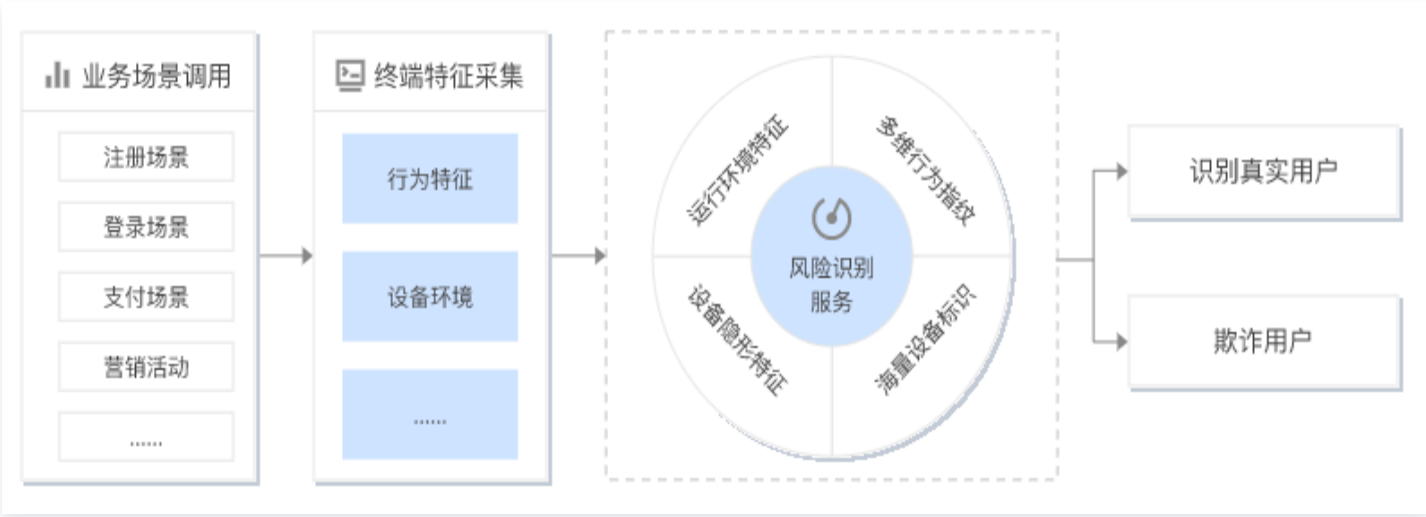
身份认证领域，黑产的攻击手法日益复杂，如人脸核身，已由之前的照片、翻拍攻击变形升级成篡改设备信息、恶意注入等更高级、更难识别的类型。同时，设备欺诈也呈多发趋势，通过 ROOT、刷机、模拟器、篡改 IMEI 等手段，伪造他人设备或身份进行业务欺诈，设备安全服务可提供身份多因子认证，多重验证保障身份安全。



扩展风控场景

以可信设备标识为基础，综合设备环境、网络环境、用户操作行为，利用 AI 机器学习和大数据技术，从机到人、多场景识别业务方在业务过程中的虚拟设备、系统篡改、应用劫持、协议破解、自动化模拟操作等各种设备风险行为，整体提升业务风控系统为各类互联网在线业务保驾护航的能力。

版权所有：腾讯云计算（北京）有限责任公司


业务场景调用
注册场景
登录场景
支付场景
营销活动
.....
终端特征采集
行为特征
设备环境
.....
运行环境特征
多维行为指纹
风险识别
服务
设备隐形特征
海量设备标识
识别真实用户
欺诈用户