

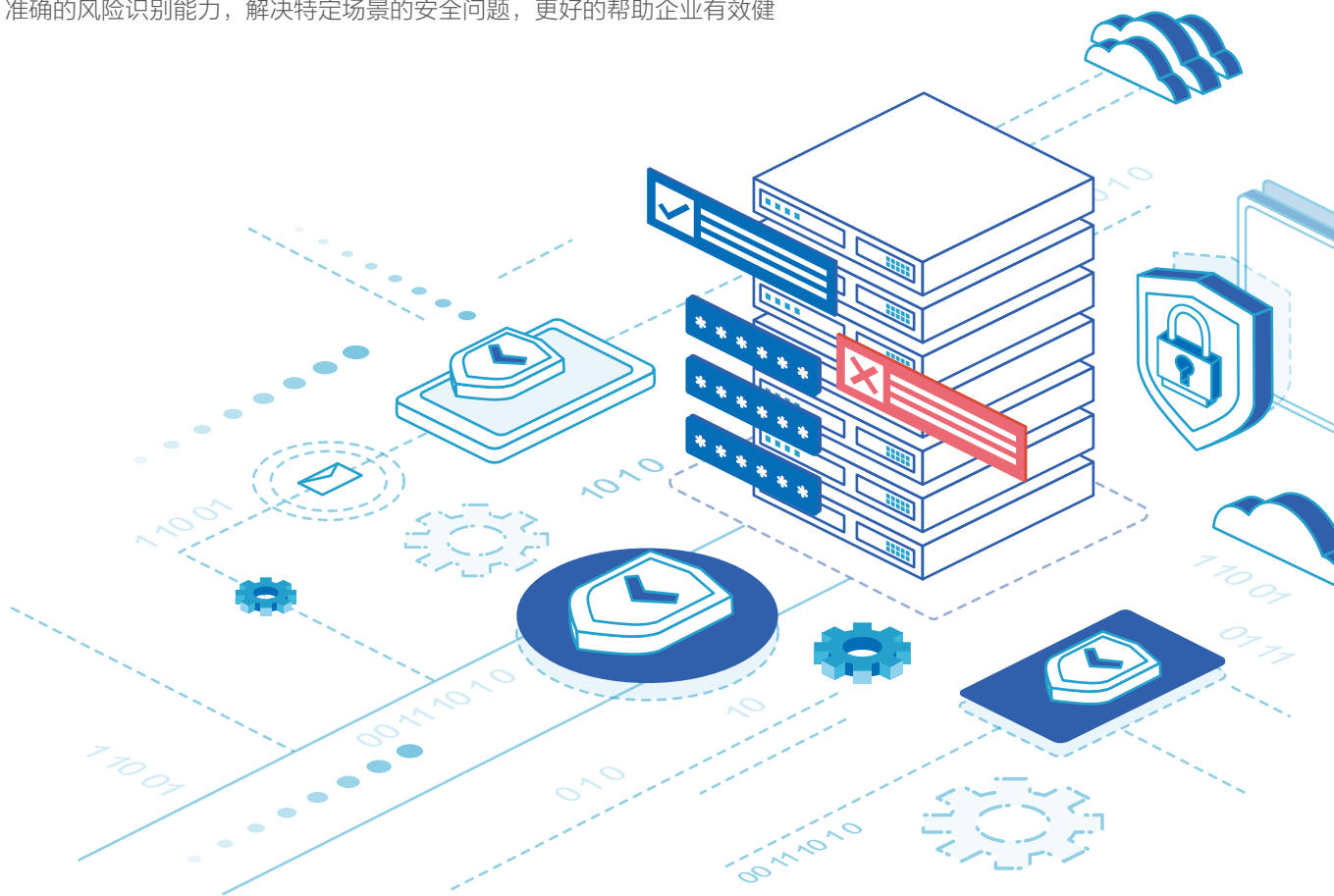
昊天镜 业务安全风险

百度安全多年打磨
业务风险管控最佳实践

产品简介

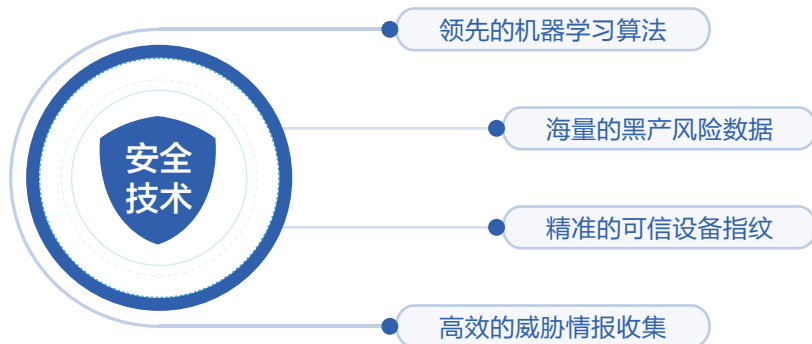
► 长期深耕互联网黑产对抗 致力于为企业打造新一代智能风控平台

基于百度领先的人工智能技术，结合海量数据，构建安全风控模型，为不同业务场景提供实时、准确的风险识别能力，解决特定场景的安全问题，更好的帮助企业有效健康发展。



业务安全场景化服务

► 融合多维度安全技术



► 深入企业各场景，构建全链路防御体系

 用户注册保护	 用户登陆保护	 营销活动防刷	 用户虚假裂变
 刷单刷券识别	 人脸识别防护	 点赞关注互动	 渠道推广反作弊
 渠道质量评级	 支付安全保障	 风险设备识别	 业务接口防刷

智能决策引擎

简介：专业的业务规则分析与管理平台，可将客户日常的业务运营决策实现自动化、智能化，并且支持不断优化。同时提供业务决策的全生命周期管理，从业务决策的挖掘开发、到决策逻辑的测试模拟、再到模型的部署上线。帮助企业快速搭建智能反欺诈引擎。

应用场景：

金融反欺诈

业务安全

支付风控

监报告警

游戏作弊

核心能力

多场景事件接入：

支持场景化事件接入，灵活管控；自定义变量管理，自动解析。多类型变量灵活扩展。

可视化策略管理：

可针对不同业务场景需求，提供自定义配置风险决策流程，实现策略可视化配置，操作简单、清晰可控，支持多种决策组件，策略更灵活。

多维度特征补充：

支持模块化多维度特征在线衍生扩充，提升决策引擎数据丰富程度。

实时指标计算：

引擎内置统计、去重累计、求和、求平均、求关联、风险趋势等丰富的实时指标计算组件。

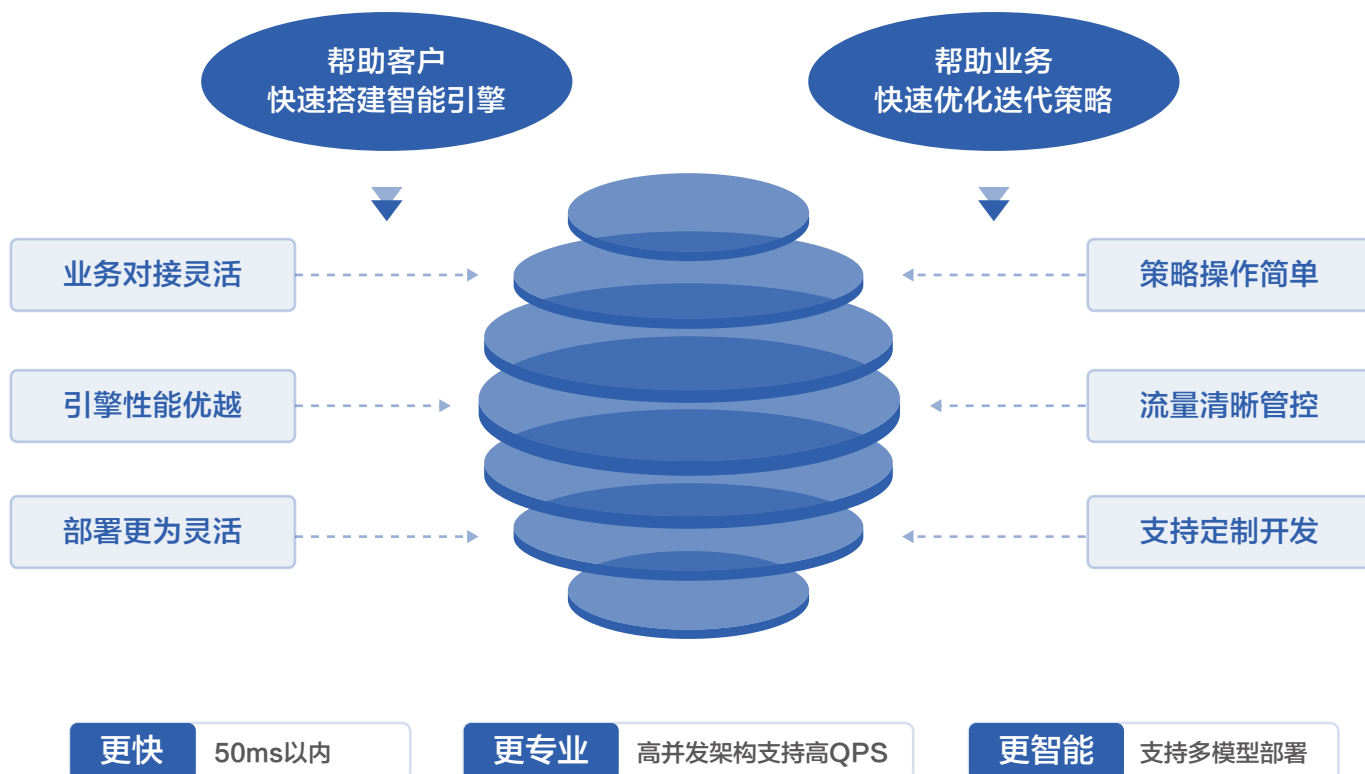
策略分析与实验：

提供策略制定，测试评估等实验室分析能力，可用于策略孵化、策略调优等场景。

智能风险监控：

提供可视化的风险大盘，风险趋势实时监控，风控请求实时查询，实现风险态势第一时间感知。

核心优势



风控蓝军平台

简介：凭借百度安全黑产对抗经验、及多维度的威胁情报，模拟黑产主流攻击手段，对业务进行全方位测评，以攻促防，提升企业黑产对抗能力，做到业务漏洞尽早发现，策略效果了如指掌，全面助力企业建立完善的风控防御体系。

应用场景：

业务上线前

业务上线前测评，提前感知风险漏洞，并提供修复指导；漏洞修复后，二次测评验证修复效果。

业务上线中

定期测评，及时修复发现的漏洞；通过平台快速模拟复现收集的黑产作弊情报，验证风控防御能力。

完善风控防御体系

持续进行攻防对抗，不断强化风控系统防御能力；专业测评第三方采购的风控工具，保障风控防御体系可靠性。

核心能力

业务安全测评：

模拟黑产攻击方式，对业务线发起自动化攻击测评，检验业务安全防护能力，提供专业修复指导。支持营销活动、账号安全、在线交易、人脸识别等多种业务场景。

接口安全测评：

对于暴露的业务接口，提供丰富的接口攻击测评能力，模拟多种接口攻击方式，评估业务接口安全防护等级。

风控工具测评：

直接对自研或外采的风控工具进行测评，如设备指纹、设备风险识别能力等，有效验证风控工具的防护能力和效果，挖掘风控工具薄弱点。

多场景测评报告：

基于各个业务场景特性，输出多维度、科学准确的评估报告，并提出漏洞修复建议，指导企业提升风控防护能力。

核心优势

引擎能力强大

基于强大的群控系统，支持数百台设备同时攻击，真实模拟黑产攻击场景

风险覆盖全面

预置数十种黑产风险，并隐藏设备风险特征，加大风控识别难度

持续攻防对抗

可与风控系统进行持续攻防对抗，指导风控防御体系升级

黑产情报支持

监控黑产业务攻击方向，给出详细黑产情报数据支持，评估风控系统黑产数据覆盖

测评流程自动化

操作简便、流程快速、人工成本低

多设备类型支持

覆盖模拟器、真机、云手机的群控操作，全面检测设备维度防护能力

智能化可信设备指纹

简介：基于百度安全能力支撑，分配全球唯一可信设备ID，识别风险设备，欺诈仿冒无处藏匿。

应用场景：

金融反欺诈

游戏反作弊

活动防刷

支付安全

人脸安全

精准营销

核心能力

设备标识

关联设备、网路、账号等多维度特征，结合百度安全多年实战沉淀的设备DNA模型算法，颁发唯一设备ID。

安全因子

主动检测运行环境，追踪系统、应用层面存在的风险和漏洞，可以有效输出包含模拟器、群控、改机、ROM注入、应用双开等在内的诸多设备安全因子。

设备画像

可以与海量设备数据关联分析，产出丰富、精准的模拟器、云手机、设备改机等纬度风险画像。

核心优势

隐私合规性

- 符合国家用户隐私合规监管，不会过度采集用户信息

纯云端生成

- 不在本地保留指纹，防止被逆向
- 百度安全特有机器学习算法

指纹云端打通

- 指纹作为主键

高度隐私保护

- 加密传输&独特算法

智能对抗

- 可主动刷新策略对抗破解

风控知识库

简介：基于百度安全与黑产持续对抗沉淀的安全因子、策略模型，精准识别各场景下业务风险，提供设备、IP、应用等多维度风险画像数据。补充合作企业黑产情报数据，建立更完善的事前风险感知能力、强化风险设备识别能力。

核心能力

风控知识库三层核心能力，全面提升企业现有风控能力。



分享裂变异常
识别模型



聚类异常
检测模型



异常行为
检测模型



风险态势
感知模型



等几十类
策略模型



模拟器



云手机



改机



应用双开



等二十余类



群控设备



设备调试



定制ROM



风险框架



风险设备库



真机设备库



风险应用库



风险IP库



等十余类
情报库

策略模型

提供场景丰富、效果稳定的策略模型，同时支持结合开发者自身业务特征，进行风控模型定制。

安全因子

指导开发者自主采集设备特征，查询风控知识库，获取xposed、群控、模拟器等安全因子及风险画像，判定设备风险，无需引入SDK。

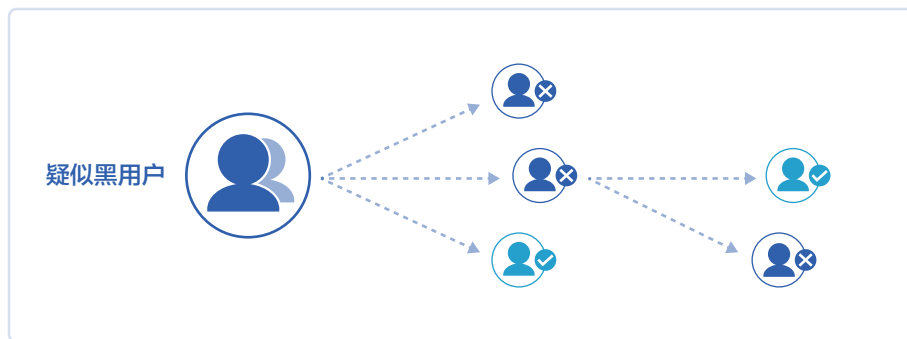
黑产情报库

提供风险IP库、风险知识库、白设备库、风险应用库、羊毛党人群库等十余类黑产情报库及标签，覆盖多种设备类型。

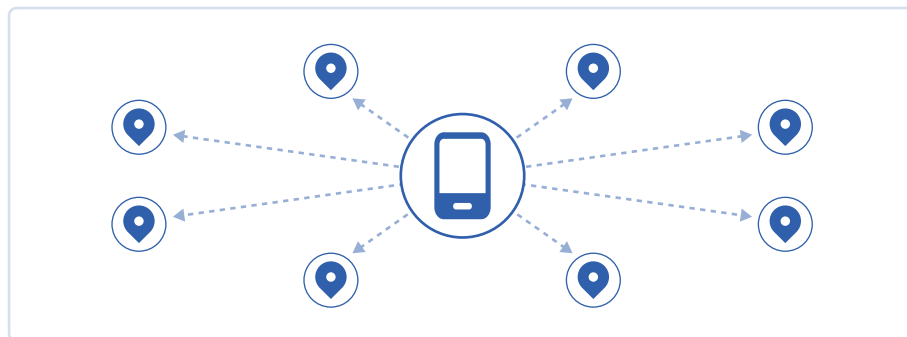
策略模型图示：



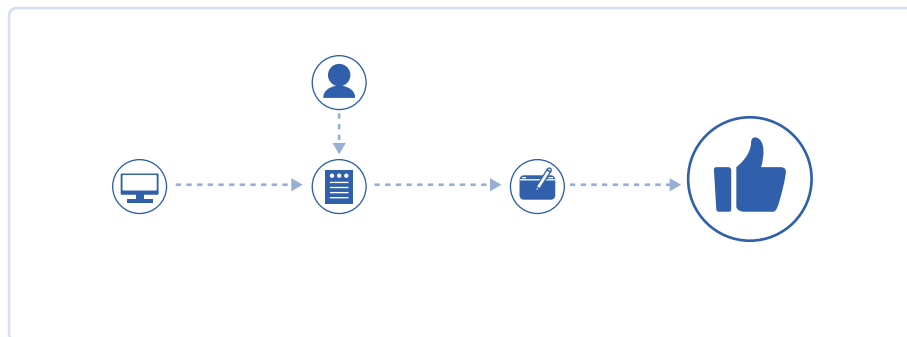
通过已知黑产关联
发现其他黑产



同一设备短时间
在多个地点出现



基于开发者业务需求
自定义模型



应用场景：

实时态势感知

企业在自身未建立风控系统的情况下，可利用知识库进行业务安全监控，实时感知业务风险。



风控体系数据扩充

开发者自身拥有风控体系时，风控团队可借助知识库，扩充黑产情报数据，更好掌握业务安全。



核心优势



数据量

覆盖中国移动设备超80%
+亿级别白设备，亿级别黑设备



无需集成 SDK

无需集成客户端SDK，可无损提供客户端风险识别能力



时效性

IP情报库分钟级更新，设备情报库天级别更新



高召回

与传统单一设备、IP情报产品对比，识别能力提升9倍

通用场景解决方案

方案架构：业务全链路实时布控，各环节风险第一时间感知处置，有效保障业务安全。



落地案例：某金融机构

► 设备指纹+人脸安全项目

业务痛点

- **风险检测要求高**——金融行业想要避免重大资损，需要准确的设备风险检测和极稳定的设备唯一标识。
- **人脸安全能力难以达标**——人脸识别作为金融行业常规的认证与支付方式，一直受到相关国家机构的重视与监管，对于人脸安全不达标的企业会限制其业务的开展。

百度方案

- **设备风险全覆盖**——在稳定的设备指纹能力基础上，有效覆盖虚假设备、改机框架、双开、群控等数十种设备风险。
- **国家级标准的人脸安全方案**——荣获中国信通院【2021年度“护脸计划”突出贡献单位】荣誉证书，参与《人脸信息处理合规操作指南》、《金融APP人脸识别线上身份认证安全能力要求》、《人脸识别系统合规能力评测规范》标准编制，提供高安全性、高通过率、高易用性远程人脸身份核验方案。

客户价值

- **业务安全高效护航**——设备风险实时感知，黑产攻击无所遁形。
- **解决方案完善**——国家级标准的人脸安全解决方案，满足一切监管要求，便捷接入，定期升级。

落地案例：某知名城商行

► 设备指纹项目

业务痛点

- **设备唯一性差**——移动端设备经过改机、应用卸载重装、系统升级后，设备特征发生变化，无法标识设备的唯一性。
- **风险识别难度大**——黑产作弊手段多样，设备风险识别难度大，业务安全无法保障。

百度方案

- **高召回，强打通**——有效识别并找回重装、清理、改机等各情况下的设备指纹，支持设备克隆识别和跨应用打通能力，有效保障设备唯一性。
- **多维度风险识别**——基于设备指纹服务，有效识别虚假设备、改机框架、双开、群控等数十种设备风险，并提供设备风险标签和设备风险评分，帮助企业完善设备风险防护能力。

客户价值

- **保障业务安全**——建立完善的设备风险标签和设备画像体系，准确识别业务中的各类设备风险。
- **降低运维成本**——接入流程快，维护成本低，定期进行便捷的服务升级。

落地案例：某大型国有银行

► 风控知识库项目

业务痛点

- **黑产情报规模有限**——企业黑产情报数据来源有限，无法建立成熟的设备风险态势感知能力。
- **过度依赖第三方SDK**——设备风险感知等能力通常依赖外采，引入第三方黑盒SDK，数据采集难以监管。
- **设备风险需持续对抗**——黑产技术迭代迅速，作弊工具层出不穷，强对抗场景需长期人力投入。

百度方案

- **扩充企业黑产情报来源**——将IP、设备等风险标签及画像数据，服务化封装，补充黑产情报数据，强化企业事前风险态势感知能力。
- **无SDK部署**——百度昊天镜提供风险设备识别参数获取源码，替代传统部署黑盒SDK的方式，数据安全自主可控。
- **多维度持续对抗**——基于历史真实对抗情况，沉淀风险设备识别能力及策略模型，有效识别设备篡改、模拟器、云手机等各类设备风险。

客户价值

扩充黑产情报库，获取丰富的风险画像数据，多场景下识别业务风险，在设备维度与黑产持续对抗。知识库部署至业务本地，无需集成SDK，数据采集自主可控。

百度智能云官网
cloud.baidu.com



4008-777-818

版本号: 220708