同盾科技反欺诈解决方案

业务场景	潜在风险	适用行业	规则举例及效果	同盾可提供的服务及价值
登录	账户盗用：欺诈分子盗取账户名、密码信息，伪冒账户真实持有者登录业务系统，进而进行交易/转账/修改资料等操作。 暴力破解密码：欺诈分子通过程序脚本和密码本，尝试多次登录系统破解用户帐号/密码。 撞库登录：当某些网站、论坛、支付系统发生信息泄露（被拖库），欺诈分子得到泄露的数据后，会尝试用泄露出的用户名、密码在目标客户网站登录，因为普通人的用户名和密码在多家平台都设置相似或相同，很容易通过目标平台的认证。	通用，基本上所有涉及到账户体系的网站、APP都会有此类需求。	1. 通过设备指纹技术获得终端用户的设备 ID，可检查同一台设备关联的账户个数是否正常，同一台设备登录次数等。通过生物探针技术可检查是否是机器脚本访问。 2. 实际客户案例效果：某一在线旅游电商客户，使用了 同盾的设备指纹服务，在一个月内就发现了多次撞库行为，及时采取了 预防措施。	同盾风险决策系统（SAAS）通过名单类规则,关联类规则,频度类规则,时间类规则,设备指纹，生物探针，代理 IP 检测等手段，可有效识别账户盗用风险，检测当前登录的账户是否被盗用，保护用户资料不被泄漏，降低由此带来的资金损失，保护平台的品牌声誉。
注册	批量垃圾注册账户：欺诈者通过脚本自动或手动注册多个账户，用于欺诈、抢红包、虚假交易、发垃圾消息等恶意行为。对于此类风险采用事后日志分析的方式几乎是徒劳的，因为风险已经发生了，没能有效的预防住。而且不采用设备指纹等技术，此类风险甚至都无法识别。 批量虚假注册账户：欺诈者购买大量虚假飞实名注册手机号注册多个账户，此类手机号只能够接收短信实际拨打电话为空号，用于欺诈、抢红包、盗卡交易等恶意行为。 ”薅羊毛”现象：“羊毛党”是指用利用各商家的优惠促销活动，以较少的成本或零成本赢取相对较高收益和奖品礼品的群体。目前一些理财平台注册即送现金红包，由于羊毛党通过大量的垃圾注册多次在同一平台获取营销红利，使得平台在市场推广上的效果欠佳。	通用，基本上所有涉及到账户体系的网站、APP都会有此类需求。只不过不同平台的垃圾注册目的不同。比如电商平台中用于刷单、抢红包、抢补贴；社交论坛中用于骗钱、灌水、发小广告、垃圾消息等。	1.通过设备指纹技术获得终端用户的设备 ID，可检查同一台设备关联的注册账户个数是否正常，同一台设备/同一 IP 是否频繁注册，注册手机号是否命中我们的虚假手机号黑名单库等。通过生物探针技术可检查是否是机器脚本访问。 2.实际客户案例效果： 某一 P2P 行业客户通过微信注册送红包的方式吸引客户注册，同时客户对接了同盾系统在注册时对同一个设备上重复注册的问题进行监控。上线首周就发现有 30%的客户有虚假注册问题，效果非常明显。	通过检测设备是否在垃圾注册黑名单中，注册来源 IP 是否为代理，在设备为空的前提下 IP 注册行为为频繁，且关联账户非常多，注册账户名相似度检测，同 IP 或设备注册账户数异常等方面，同盾可以助企业有效地检测垃圾注册风险。
交易	盗卡支付：欺诈者使用盗用的信用卡，银行卡在互联网金融、电商、航空商旅、游戏等平台上进行支付，平台面临持卡人拒付风险和声誉的损失。	电商、O2O、商旅、支付、游戏等行业。	1.同一设备是否存在全局欺诈库盗卡欺诈事实；同一设备绑定银行卡数目；交易速率是否正常。 2.实际客户案例效果：	通过大数据的规则模型和实时风险决策系统，结合基于设备指纹的机器识别技术，同盾科技可以帮助企业识别盗卡支付风险和虚假交易风险。发现机器设备,IP,卡是否存在欺诈事实风险，同一张卡支付发生的移动速率是否正常。通过有资金交易关系的账户，设

			某支付网站，利用同盾的强大的规则引擎，非常方便的实现业务规则配置。同时同盾强大的计算能力，可以在极短时间内进行运算处理，实时返回计算结果。	备网络拓扑分析，发现潜在的存在虚假交易的主体。
	虚假交易：在电商平台中，卖家与买家合谋，通过虚假交易炒作卖家信用、套现盗用的银行卡。带来的危害包括：消费者难以判断优质商户,商户的竞争变成恶意竞争,电商平台的信用评价体系遭到破坏,长久下去对平台品牌形象造成严重破坏。在一些 O2O 平台，也存在通过虚假交易刷单，赚取平台补贴的情况。	电商、O2O、商旅等行业。	1.商品数极多且单价不正常；买家关联的卖家个数很少；短时间内同一设备发生交易次数频繁，且不断切换 IP 地址。 2.实际客户案例效果 某 O2O 平台，利用送红包形式进行营销，最多一周的红包赠送量超过百万，但是发现其中有很多刷单骗取红包的行为。使用了 同盾的服务，接入后一周就发现了 超过 50%的作弊行为，为客户避免了大量不必要的支出。	
账户提现	在互联网金融业务中，投资人或借款人都可能面临异常提现的风险。当账户被盗用后，账户中的资金被恶意提取到欺诈者的银行卡卡或账户中。	理财、基金销售平台、P2P 等	1.提现是否为常用设备；设备提现时间、频度。 2.实际客户案例 某 P2P 平台的一个客户，发现短时间登录的地区发生变化，一个小时内原先由北京登录，改为了广州登录，且登录后修改绑定银行卡并且提现。平台发现情况后，及时与客户联系，确认非本人操作，为客户防止了损失。	通过检测提现时是否为用户常用设备/浏览器/登录地/IP，提现时间，提现频度，提现卡号等维度，同盾风险决策系统可以有效检测出用户异常提现风险。
APP 推广营销	在积分墙等营销推广活动中，欺诈者通过多次重复激活下载 APP,骗取推广费，企业未达到推广目的,却要浪费高额的推广费用	APP 类客户	1.同设备重复激活；同网关一天超上限；Ip3 时间规则。 2.实际客户案例 参考交易案例，通过设备监控	同盾的解决方案基于决策树的规则筛选算法，通过时间相关的规则，频度相关规则，特征关联规则，类别变量规则和名单类规则，可以有效防范积分墙类营销推广中的欺诈风险。
模拟器识别	欺诈者通过在电脑中安装安卓手机模拟器，在模拟器中安装目标客户的 app，进而进行刷单、注册、抢红包、刷单交易等操作，给客户带来资金损失。	电商、O2O	通过识别是否符合模拟器的相关特征	同盾的解决方案针对模拟器特征识别配备了模式识别算法，通过应用层特征、安卓系统层特征、操作系统特征、模拟器结构特征等来识别。
抢红包营销	在企业新业务营销推广中，常常使用抢红包的方式，但一些欺诈者往往利用业务规则漏洞，通过程序脚本疯狂地抢红包，或是低价抢购营销商品后转手卖出，使得目标客户未抢到红包，企业的营销目的无法达成，业务推广受阻。	电商平台、O2O、P2P、理财等	1.人机识别，区分机器脚本抢补贴。设备指纹信息是否能够采集到。 2.实际客户案例 某电商平台推出秒杀活动，但是发现活动很多商品被黄牛在	由于机器没有“自然人”的思维及行为模式，即使进行模拟、伪造，成本也相当高。同盾的生物探针技术可以准确地识别出没有“自然人”行为特征的机器行为。可以有效判断抢红包的参与者是“人”还是“机器程序”。

			极短的时间内秒杀。引入同盾的设备指纹和生物探针服务，通过对客户的页面浏览、鼠标点击以及键盘敲击等操作的规则设置，将黄牛利用机器进行秒杀的活动轻易识破。	
借款	异常借款：中介申请，同一设备或 IP 地址发起大量申请。 失信借款：借款者身份证、手机号、邮箱等信息命中我方失信名单，曾经在其他平台中发现失信逾期不还行为。 多头借贷：同一借款人在多家平台申请借款 催收应用：申请贷款行为完成后，借款人没有还款意愿，从而导致了平台与客户的失联，欠款无从追缴。	P2P、消费金融、消费信贷、信用卡网申	1. 同一设备绑定多个身份申请；失信名单（身份证/手机号/邮箱/IP/座机）;同一身份证在多个平台借款。 2. 实际客户案例： 目前 P2P 客户利用了 同盾的黑名单检测服务，每周的命中率为 3%-5%左右，曾经在一周为某一客户在借款端拦截下来的金额接近 80 万。	同盾独有的设备指纹技术可以在消费信贷风险分析中具有较大的优势，平台在对用户做放款行为时，可以在页面中嵌入同盾的设备指纹代码，获取用户的设备信息（非用户隐私信息）。同盾建议平台对此类贷款用户务必进行信息搜集，包括不限于：用户身份信息、用户日常手机号、电邮地址、QQ、商品收货地址、用户会员信息、家庭成员、紧急联系人等信息，以便同盾的做大数据分析。同盾的全局联防联控数据可以为行方的反欺诈带来较大的帮助，由于同盾风险决策系统接入了多家 P2P、电商、支付等多个行业的客户，这些客户有着相似的用户群体，同盾可以利用全局欺诈大数据帮助某发现潜在的欺诈风险。如该用户曾经在其它相关平台有过不良信用操作，可以及时告知合作方做好防范的工作。同盾的风险决策系统服务已经内置了大量的欺诈行为检测模型，在系统中针对 P2P 借款业务、理财业务、信用卡业务配置相关规则模型，用户的每一次申请贷款行为都会经过同盾规则模型的分析，有效的对欺诈人员的交易进行监控。