通付盾
PayEgis

新互联网时代的安全专家
Security Expert of New Internet Era

暗战：营销反欺诈攻防

开放 · 诚信 · 效率 · 共赢

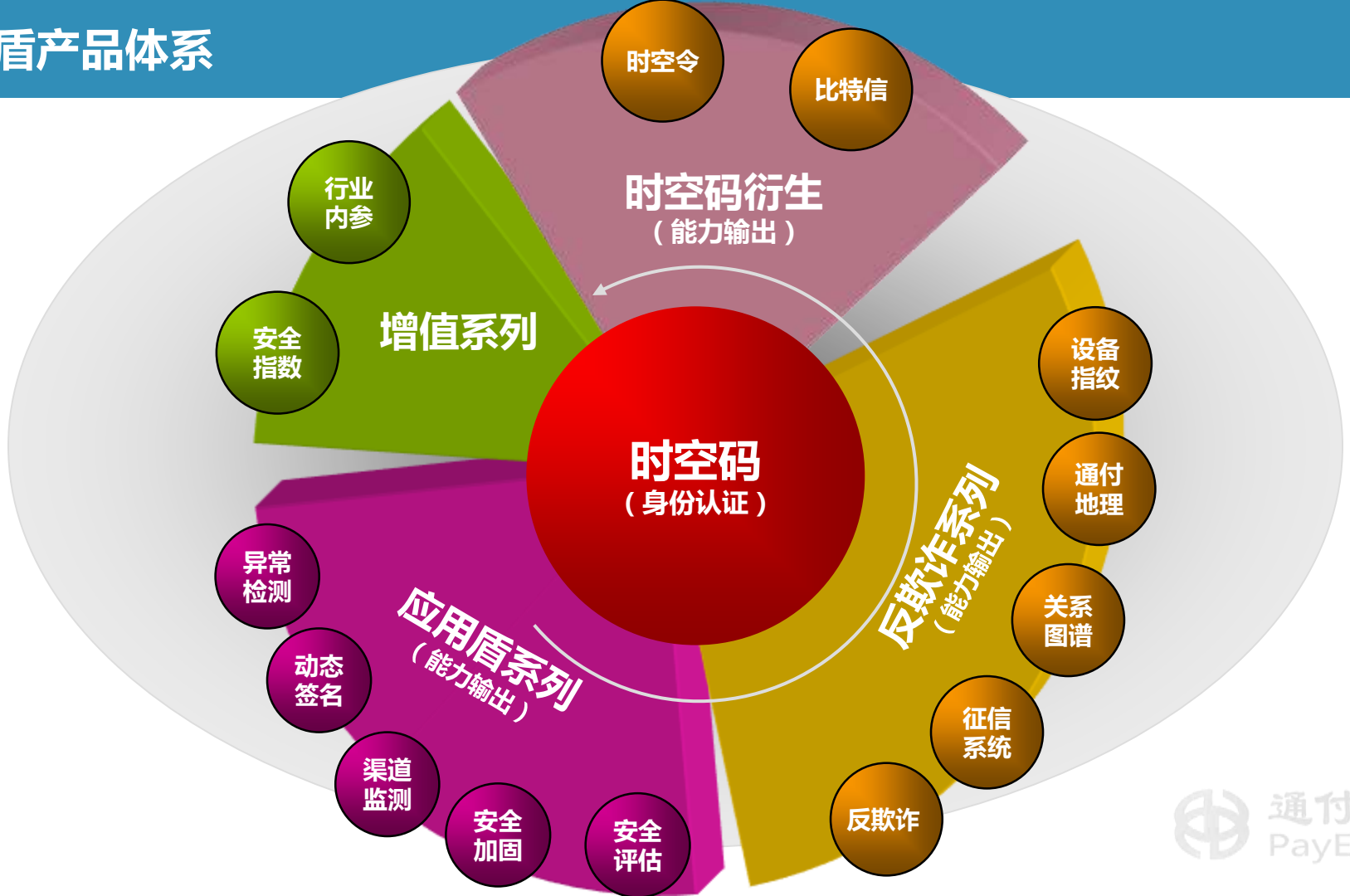
北京 • 苏州 • 杭州 • 硅谷
地址：苏州工业园区新平街 388 号腾飞创新园 6 号楼
联系邮箱：info@payegis.com
官网：www.payegis.com

Dejia Wang

Founder, Chairman and CEO, PAYEGIS

Dejia Wang is the founder of PAYEGIS and has been the Chairman and CEO since 2011. Dejia founded PAYEGIS with the singular vision of empowering consumers and consumer-facing businesses to win the war on mobile, account and transaction fraud. Mr. Wang gained more than a decade of experience working with consumer and transaction data and generating business insights out of big data. From 2001 until 2006, Mr. Wang worked at the leading CRM company Siebel Systems (acquired by Oracle), where he served in various engineering and management positions in US. From 2006 until 2011, Mr. Wang held senior architect and director level positions at Supply Chain Planning, Monetization-As-a - Service and Predictive Marketing Analytics startups: TrueDemand (acquired by Acosta), PlaySpan (acquired by VISA) and M-Factor (acquired by DemandTec, then by IBM).Mr. Wang is also a founding member of Lyris next-generation multi-channel Marketing Optimization Platform. Mr. Wang received PhD in Mathematics from University of Wisconsin-Madison, MS in Computability Theory from Institute of Software, Chinese Academy of Sciences, and BSs in Probability and Statistics, Economical Management from University of Science and Technology of China. Dr. Wang has dozens of patents pertaining to data insightand fraud detection technologies.

通付盾产品体系



目录

通付盾 PayEgis

新互联网时代的安全专家

Security Expert of New Internet Era

移动营销趋势

2012 转发抽奖（传播）

- 优点：操作简单
- 缺点：可玩性差、扩散范围有限

移动化

2013 点赞有礼（交互）

- 优点：操作简单
- 缺点：可玩性差

社交化

2014 游戏营销（好玩）

- 优点：可玩性好、扩散性好
- 缺点：成本高，对流程、美工设计要求高

游戏化

移动营销风险

移动化

社交化

关系简单、操作简单

账号简单、密码简单

游戏化

实时反馈、逻辑复杂

用户低门槛 开发高门槛

营销欺诈

线报屋 XIANBAO5.COM 分享活动线报 精彩网络生活

Baidu 贴吧

赚客吧 有奖一起赚!

bbs.zhuankebar.com 赚客之家

通付盾 PayEgis

欺诈产业链

营销成本

刷奖程序

道具

代充

金币

黑客

投入成本无法达到营销目的

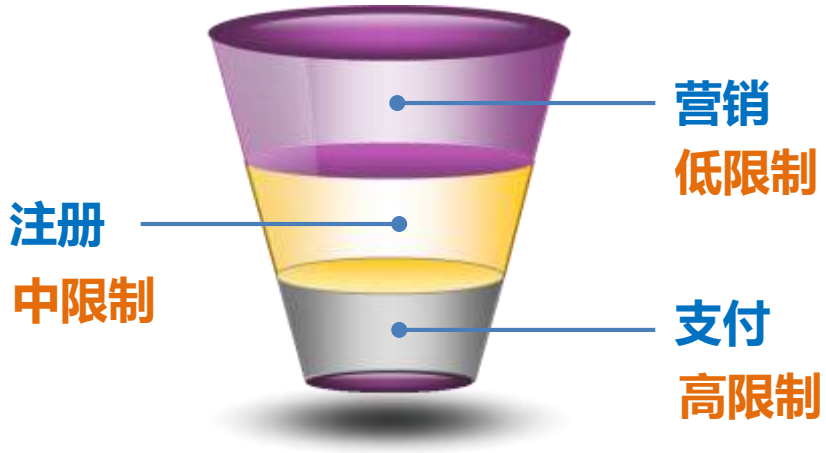
目录

通付盾 PayEgis

新互联网时代的安全专家

Security Expert of New Internet Era

案例：某股份制银行 – 推广类营销



活动详情

1、基于（微信平台）抽奖、转发好友获奖
2、奖品类型：手机话费，极易受到欺诈攻击
3、无法验证手机号码，无需关注官方微信账号
4、银行员工推荐、转发数量纳入年底绩效考核指标

欺诈威胁

黑客欺诈

首次上线24小时刷走2.5万份奖品，兑换率超过70%，活动被迫关闭，支付应用限制失效

内部欺诈

三万余名员工绩效考核压力，容易产生绩效作弊，需要进行防范

用户欺诈

普通用户可以通过更换手机号码增加获奖几率，手工刷奖用户属于非目标客户

欺诈画像

1

有时间

手工输入多个号码

2

有工具

录制、修改脚本刷奖

3

有脚本

直接写脚本通过接口刷奖

4

有资源

多台设备、多个IP（代理等）

5

懂风控

试探、绕过风控规则

一场暗战即将开始……

七种武器

规则引擎（规则说明）

条件

1、支持多种规则类型，包括计数、时间等
2、支持多种不同参数类型，支持正则表达式

操作符

1、支持逻辑操作符，“与”、“或”关系
2、支持规则层次，多个规则并发使用

动作

1、支持自定义访问决策，例如记录日志等
2、支持触发操作，模型与规则相结合

规则类型

1 速率（Velocity）

控制参数操作速率，最高精度支持分钟级别

每小时每IP访问不能超过50次

2 模式（Pattern）

定义多个参数间存在的关联，防止伪造参数、控制语义

每分钟每个IP不能超过5个设备

3 计数（Count）

定义多个参数之间的计数关系，增加参数协同控制能力

每IP进入中奖页面不超过3次

4 信誉（Reputation）

按参数类型（设备、IP等）单条规则限制信誉值

设备信誉值超过0.6才能新创建虚拟交易

5 上下文（Context）

定义单个参数的定义，支持正则表达式

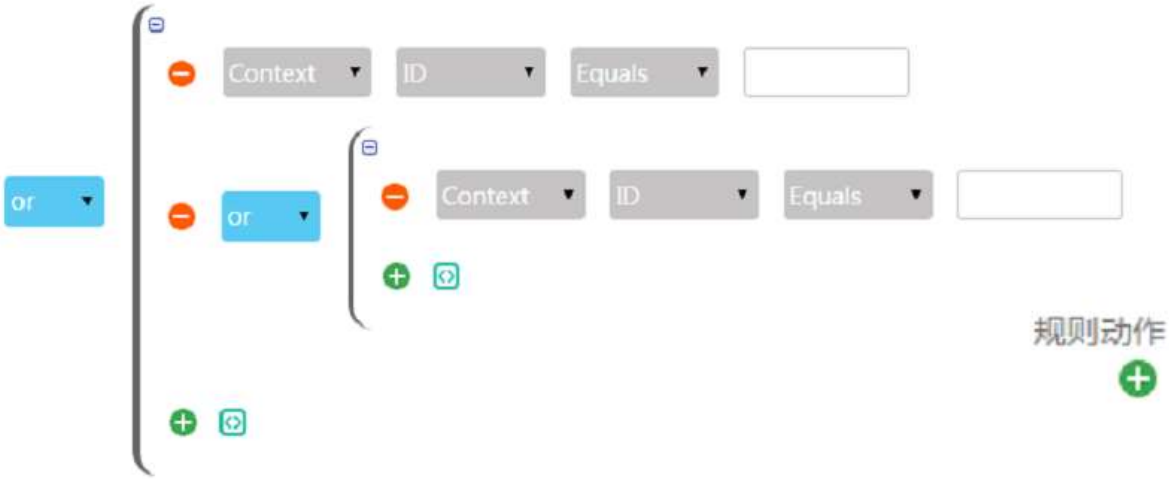
手机号码满足号段正则要求

6 统计（Stats）

根据参数的统计数值实施控制，包括最大、最小、平均、方差等

用户每日平均交易限额不超过1000元

组合示例

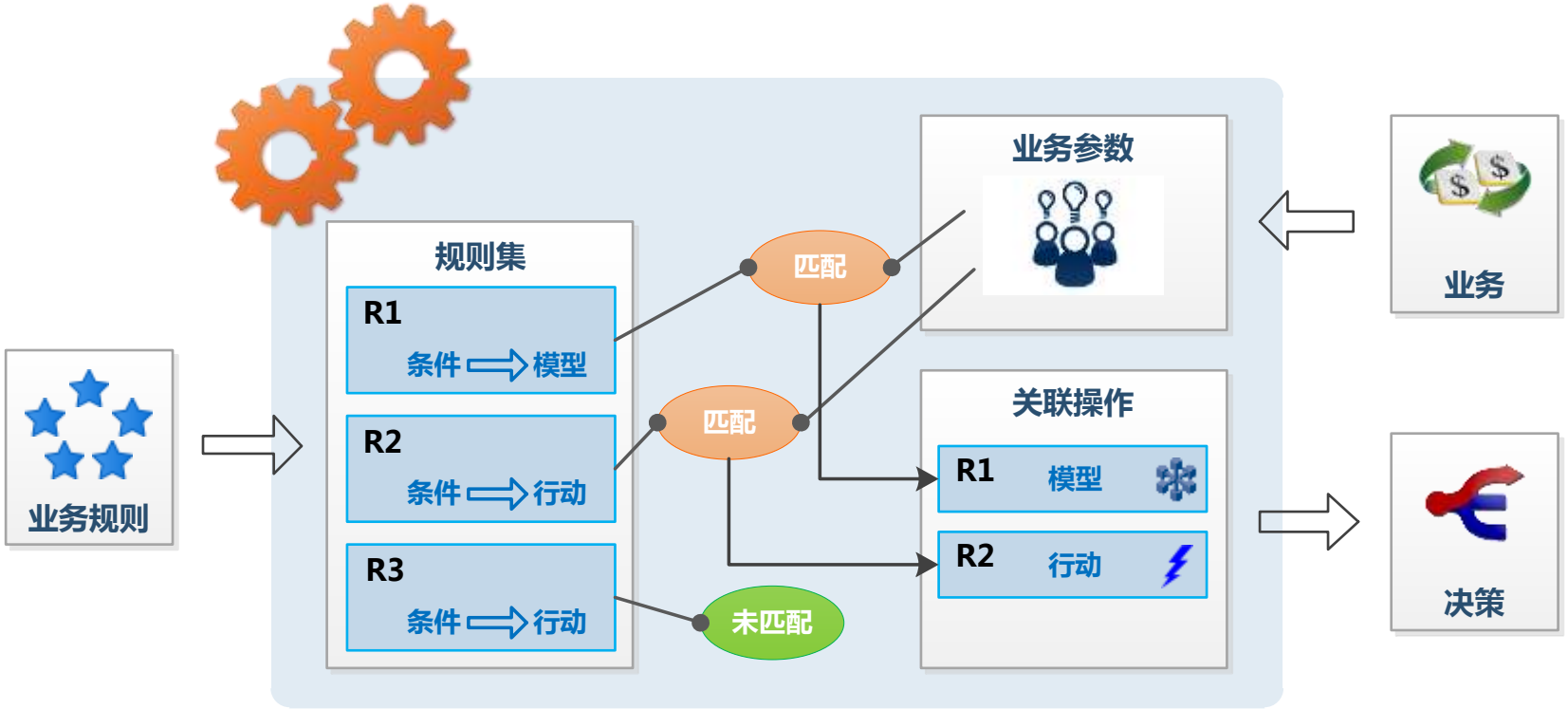


操作符组合

规则动作

动作组合

规则流程



规则引擎支持不同规则组合，实时性能响应，扩展海量并发请求

FAILED

Level1. 控制中奖次数（手工刷奖）

通付盾基于国际领先的设备指纹技术为上网设备生成唯一的ID

- 综合设备硬件属性、软件属性和行为属性
- 针对设备，不针对用户，不侵犯用户隐私

跨浏览器：同一设备多个浏览器唯一
跨平台：移动应用和移动浏览器唯一

Count规则
单参数控制

同一设备一周最多中奖5次

同一设备一天进入2次非法页面

FAILED

Level2. 录制、使用脚本（PC/模拟器）

通付盾基于国际领先的设备指纹技术为上网设备生成唯一的ID

- 综合设备硬件属性、软件属性和行为属性
- 针对设备，不针对用户，不侵犯用户隐私

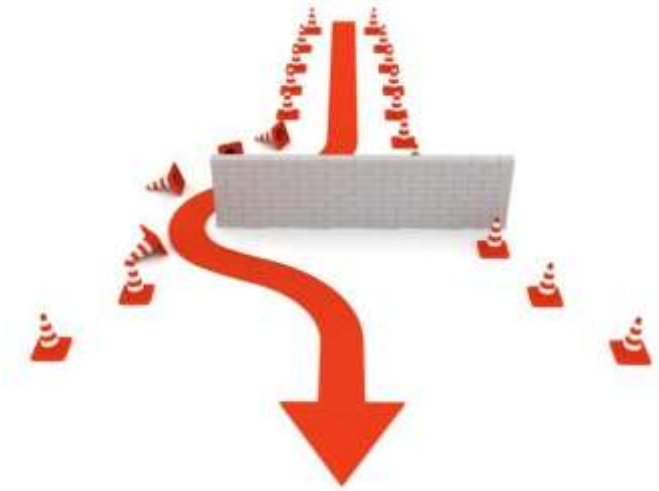
跨浏览器：同一设备多个浏览器唯一
跨平台：移动应用和移动浏览器唯一

Context规则
单参数控制

✔ 禁止PC端访问

✔ 禁止模拟器访问

FAILED Level3. 直接访问抽奖接口（脚本）



使用接口访问：

× 破坏参数的合法性：某些参数需要满足一定的限制条件

× 破坏流程的合法性：流程中多个步骤的参数之间存在关联

伪造参数：

× 自动触发黑名单：满足规则自动加入黑名单

Context规则触发单参数控制

✔ 设备指纹不合法拉黑

✔ 链接ID仅出现一次就中奖

FAILED

Level4. 多IP地址/使用代理（IP资源）

通付地理（GeoIP）拥有完备的全球IP地理信息大数据库，能精准识别任意IP地址所对应的详细地理位置

- 快速、准确的定位
- 毫秒级的响应
- 代理/VPN IP库

黑白名单
单参数控制

- ✔ 禁止使用代理服务器
- ✔ IP地域和手机号段不匹配

FAILED

Level4. 使用多个资源（号码/IP）

比较关联参数之间的相似度

× 例如：手机号码

- 13901234567
- 13901234568

× 例如：IP地址

- 202.112.58.200
- 202.112.58.142

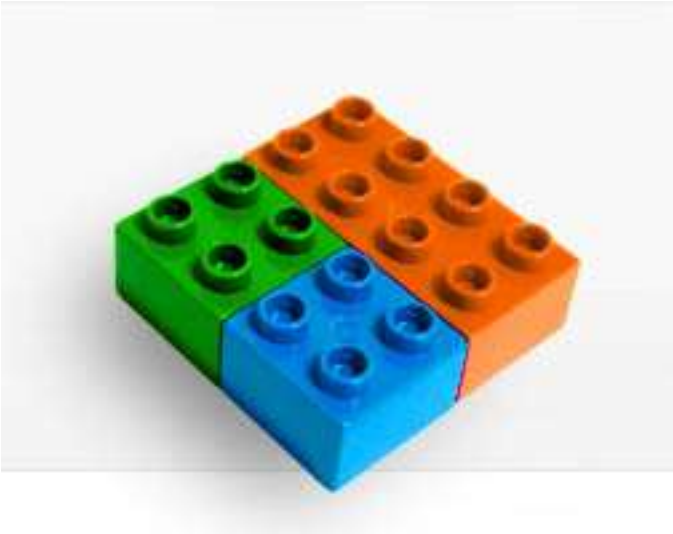
Similarity规则
单参数控制

✔ 号码有效性正则表达式匹配

✔ 30分钟内相似号码统计

FAILED

Level4. 多参数组合使用（号码/IP/设备）



参数之间存在关联关系，通常限制一段时间内一个参数与其他参数映射关系。例如当天一个设备对应的账号数量不能超过5个、1小时同一账号对应的转账次数不能超过5次限制等

Pattern规则
多参数控制

同一设备当天对应3个以上号码

FAILED

Level5. 微调参数

× 每次请求的多个参数中，仅修改少量参数，试探反欺诈规则

× 信誉管理：各参数（账号、IP、设备）具有信誉值，累积计算总信誉值，设置规则控制

Reputation规则
单参数控制

✔ 禁止信誉值小于0.5设备访问

✔ 拒绝一次信誉值降低0.05

Level5. 好甜的蜜罐（设备指纹/抽奖页面）

FAILED

对已识别刷奖行为的操作，仅拒绝容易促使黑客变化策略，加重系统负担。

× 自定义标签（例如honeypot）
× 与业务系统联动，例如发现伪造设备指纹、设备黑名单，将其引入蜜罐服务器，仅显示静态页面无法中奖

Level5. 其他

根据时间区分限制程度，例如正常操作少的夜间实施更加严格限制

重复奖品检测，应用Bug导致的一个奖品发放给多个用户

Time规则
单参数控制

Count规则
单参数控制

- 10PM-6AM严格限制
- 奖品出现超过1次，执行RETRY建议（自定义）

分析模型

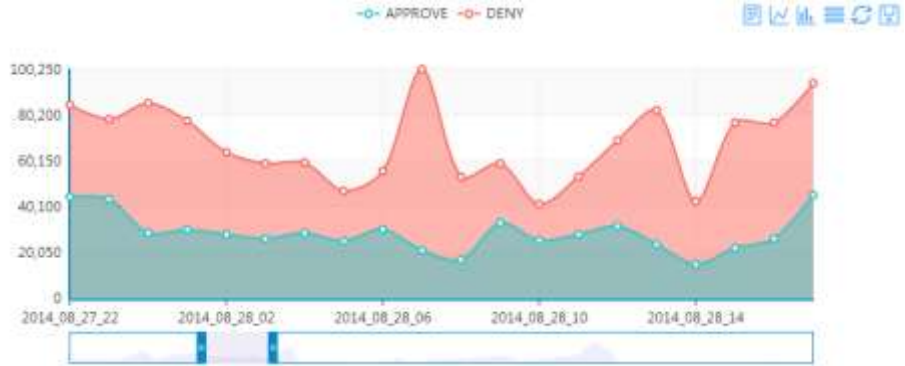
风险分析模型对地区、业务、客户分布等不同，通过大量数据的分析，对模型结构、特征指标和参数进行训练，选择最适合的欺诈检测模型

- 商户特征分析模型
- 商户行为分析模型
- 持卡人特征分析模型
- 持卡人行为分析模型
- 专家经验知识
- 欺诈历史数据
- 数据仿真
- 数据分析与挖掘算法

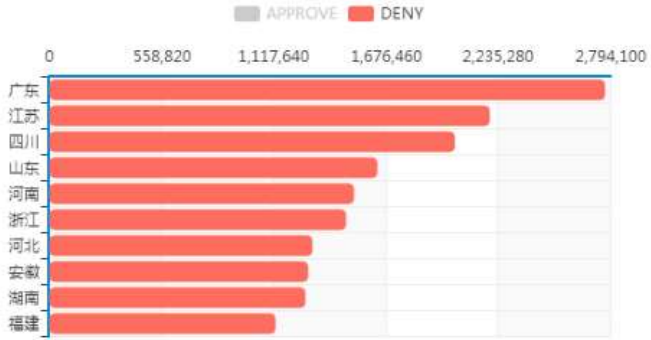
设备征信

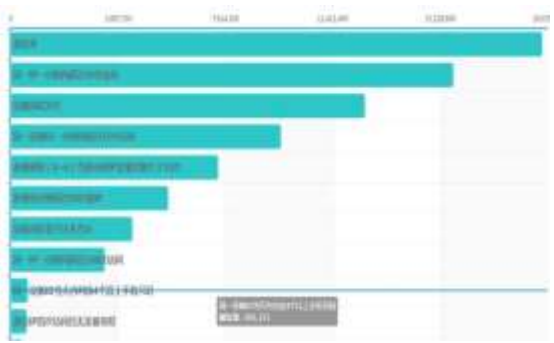
- 基于设备的信誉测评系统
- 多维度设备信誉库及设备习性库进行大数据分析
- 从设备涉及的交易记录、安全性能、病毒抵抗能力等多个维度
- 为企业、金融机构等提供设备信誉分析

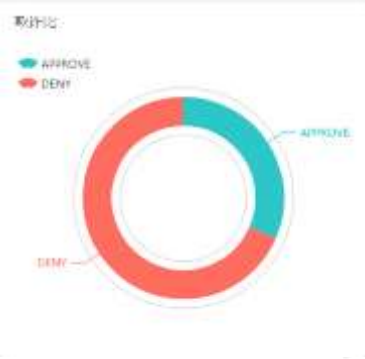
数据展现



高风险地区







通付盾
PayEgis

新互联网时代的安全专家
Security Expert of New Internet Era

招募战友

开放 · 诚信 · 效率 · 共赢

北京 • 苏州 • 杭州 • 硅谷
地址：苏州工业园区新平街 388 号腾飞创新园 6 号楼
联系邮箱：info@payegis.com
官网：www.payegis.com