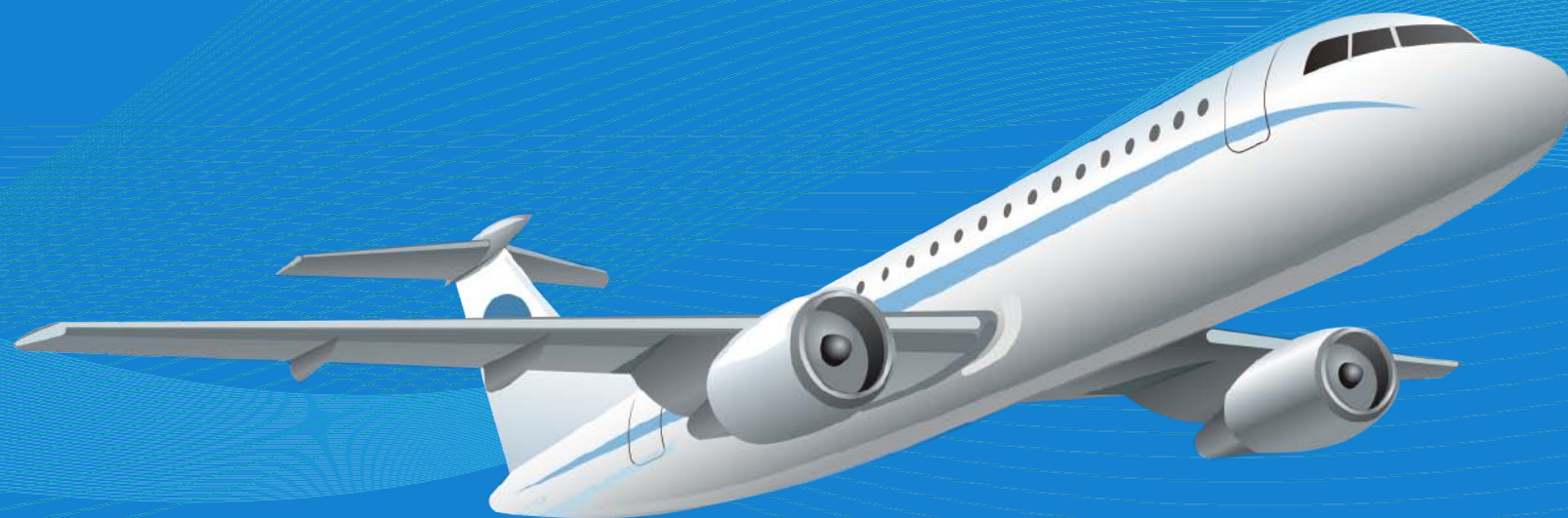


# 人工智能 助力民航票务业务安全



## 提直降代

### 收入

提升收入  
降低成本

### 增值服务

旅游, 酒店  
其他商品  
联名服务

### 用户属性

属性分析  
需求预测

### 用户粘性

高价值用户  
高频次用户

## 电商 业务安全

### 爬虫

IT资源  
业务复杂  
影响用户体验  
航信查询费

### 黄牛占座

紧缺资源被占  
提高成本  
空座损失

## 提直降代

15年国资委开始要求航空公司提升机票直销、降低代理分销，简称提直降代。从这几年的情况来看其实效果并不明显大家普遍更愿意通过携程、飞猪等平台来订票。

- 原航空公司的官网往往因为只剩高价票
- 用户体验差，反应慢，操作繁琐，有些为了省验证码居然要验证码的验证码
- 没有做宣传投放



**基本信息**

- \* 称谓: 请选择
- \* 中文姓: [input field]
- \* 中文名: [input field]
- 姓(英文-拼音): [input field]
- 名(英文-拼音): [input field]
- 邮箱: [input field]
- \* 证件类型: 请选择
- \* 证件号: [input field]
- \* 生日: 身份证中间为默认
- 密保问题: 请输入密保问题
- 答案: 请输入密保答案

**通讯信息**

- \* 地址类型: 居住地址
- \* 国家: 中国
- \* 省: --中国必填填写--
- \* 市: --中国必填填写--
- 邮编: [input field]
- \* 手机: [input field] 请填写
- 固定电话: [input field]
- 单位名称: [input field]
- 职位: 职员
- \* 联系语言: 简体中文
- \* 接受推广邮件: 是



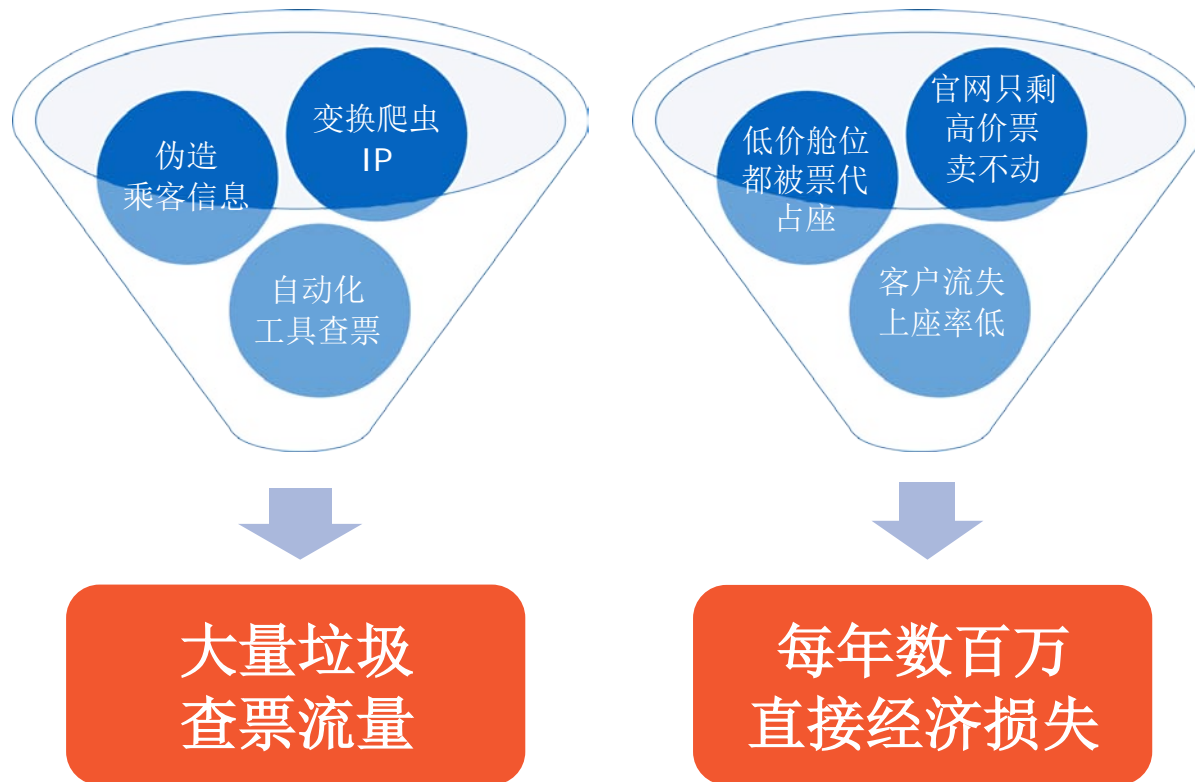
Your connection is not private

Attackers might be trying to steal your information from [www.csair.com](http://www.csair.com) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_SYMANTEC\_LEGACY

## 电商业务安全

即查询和订票的比例。查询是耗费资源的，包括网站前端资源占用以及底层服务调用产生的费用；预定是有收益的，当平均到每个预定的查询资源消耗超过了一个预定产生的收益，那这个预定就没意义了，不赚钱了



- 互联网，移动话联网时代：用户体验优先，**攻防节奏加快**
- 传统安全：周期长，误报率高，成本高，无法支持业务安全诉求

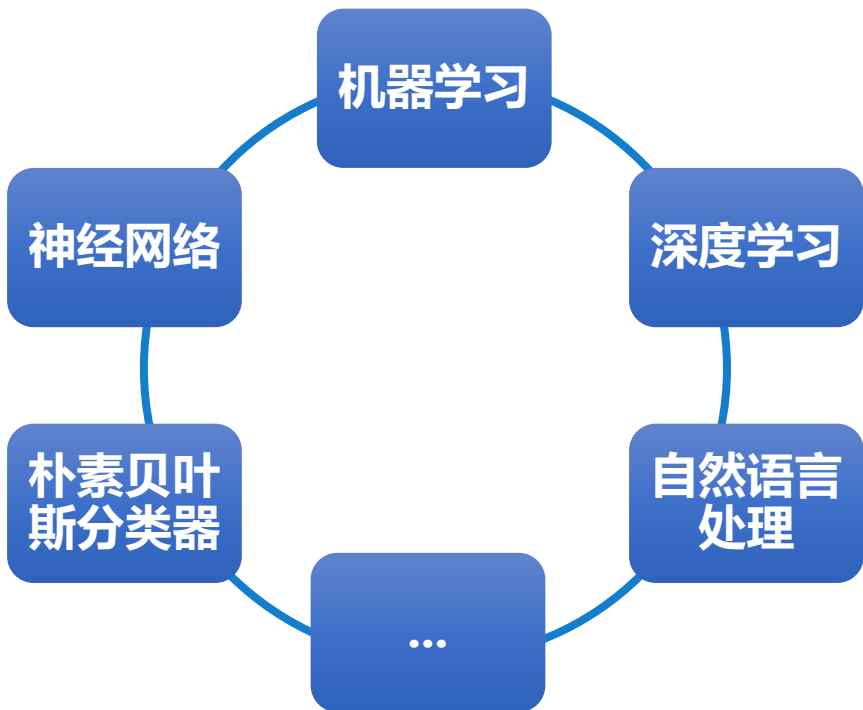
## ▶ WHY? ◀

- 依靠行业经验制定反欺诈策略，强依赖于专家知识全面性
- 人工生产的规则实效性差，无法快速响应新型欺诈特征
- 传统的驻场，需求变更，实施流程安全方案周期长、费效比低



# 人工智能助力民航票务安全





十年来，AI在深度学习、机器学习和自然语言处理方面取得很大的进展，



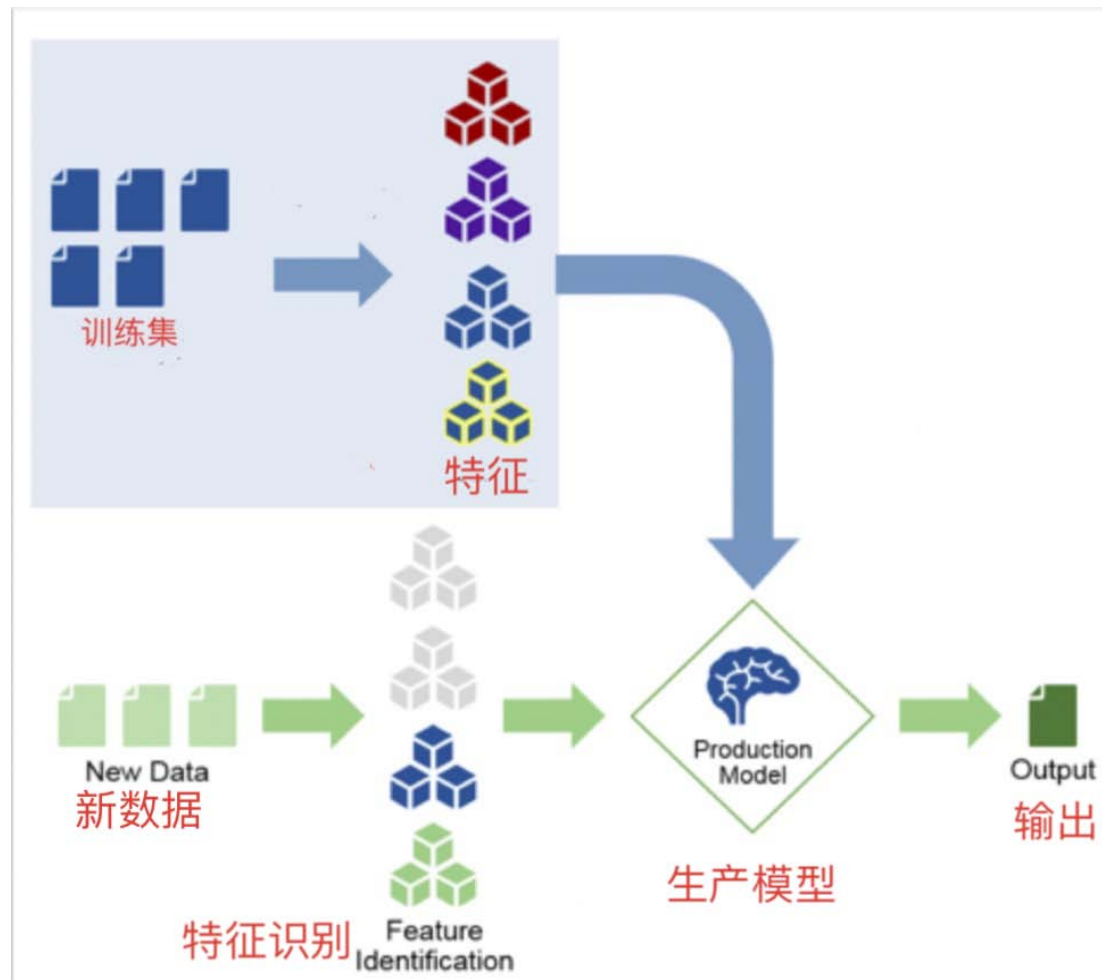
AI技术已从小众科技领域提升到主流商业软件领域，



AI技术已经成为安全研发运维环境和防护领域中的有力工具

## AI从大量数据训练开始

通过训练，最终确定特征参数，成预测模型  
验证模型预测的精度并持续训练直到模型足够精确。

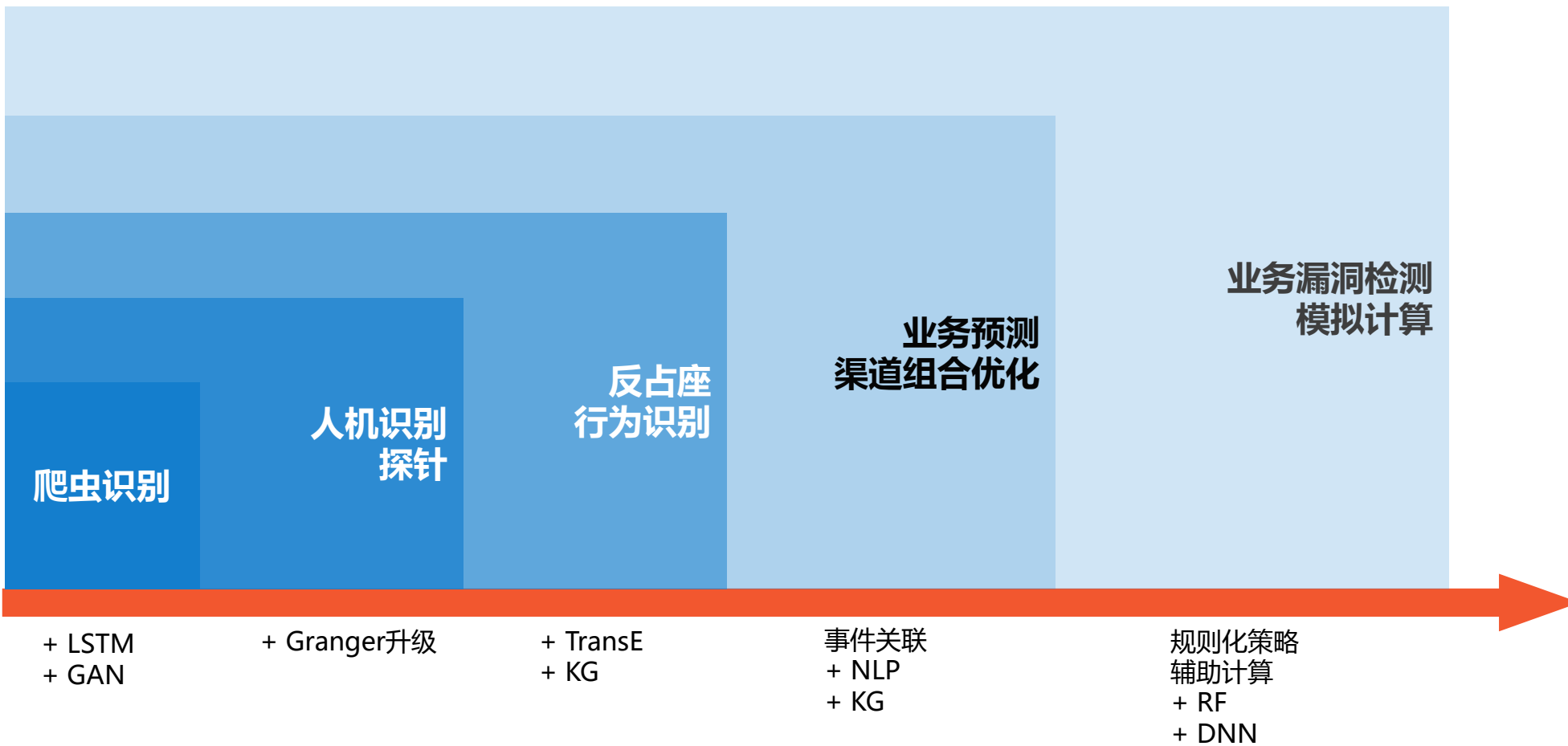




见所未见

知所未知

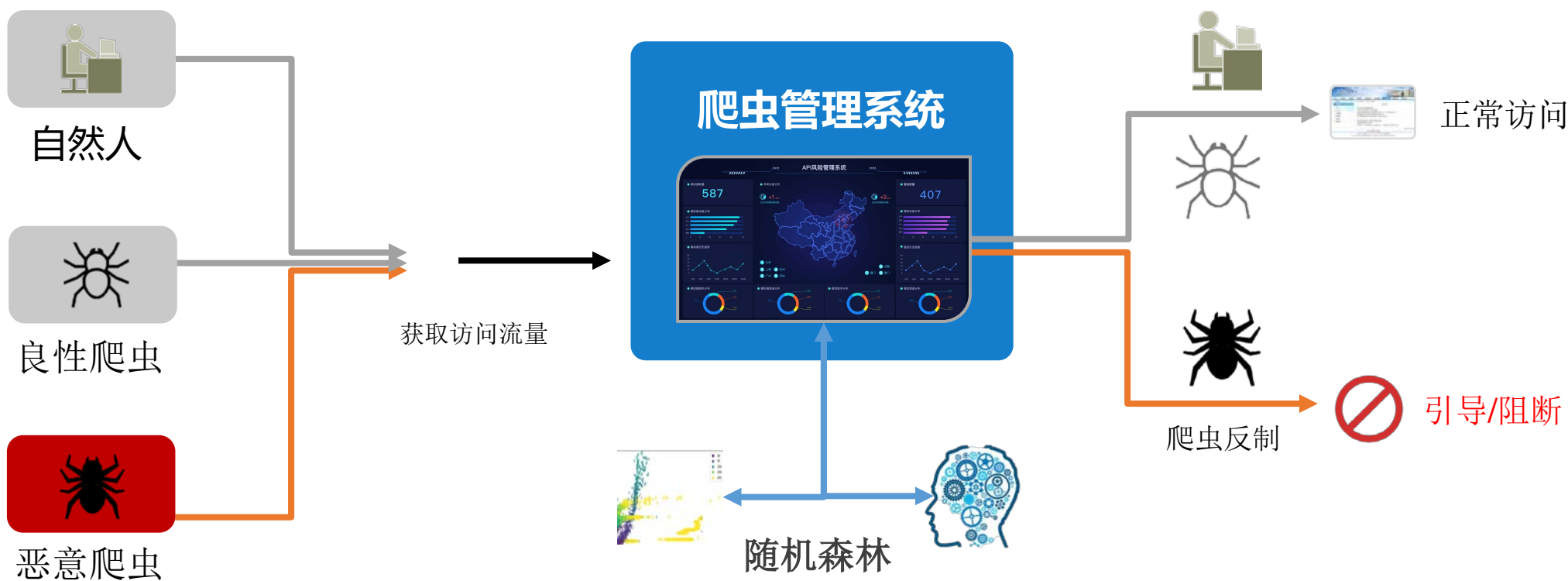
防所未防



# 见所未见：识别不同的爬虫

传统的防爬技术的核心是识别爬虫和及阻断，但是**识别请求是否来自爬虫毫无意义**，只要满足查订比甚至可以**默认大部分请求来自爬虫**  
问题的关键是通过爬虫的行为判断：

1. 可能带来业务的爬虫
2. 可能成单率较低的恶意爬虫



## 随机森林

1

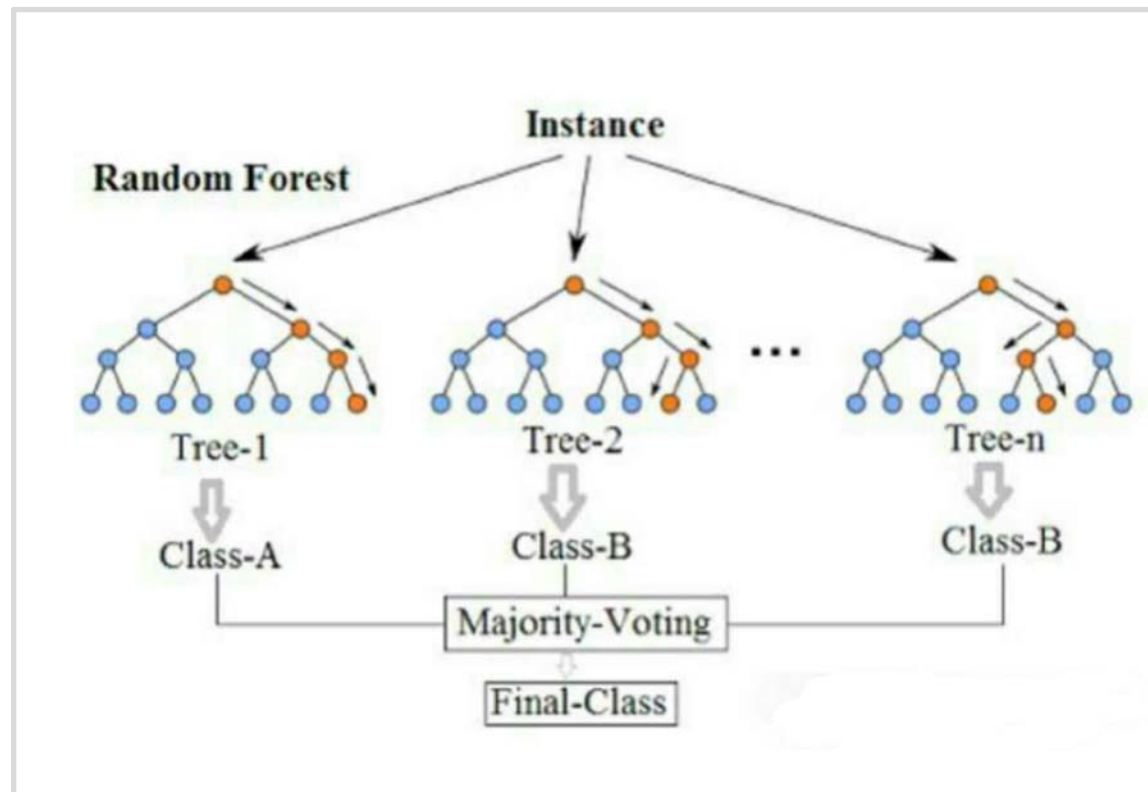
不同航段，起飞时间/座位属性/人物属性是时刻变化的庞大数据

2

爬虫的行为是一直变化的，存在不稳定性和人类不可感知

3

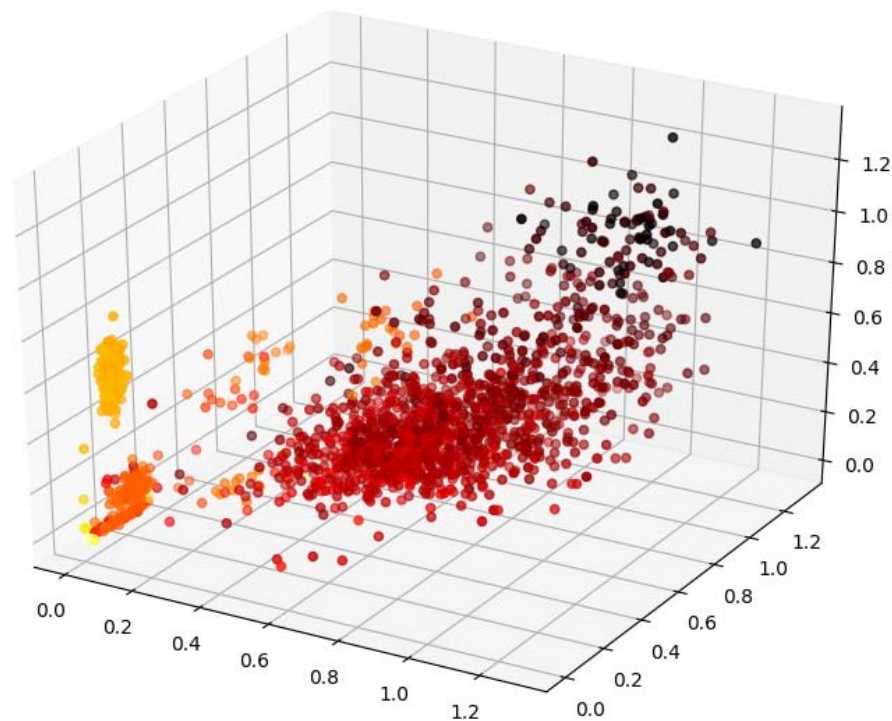
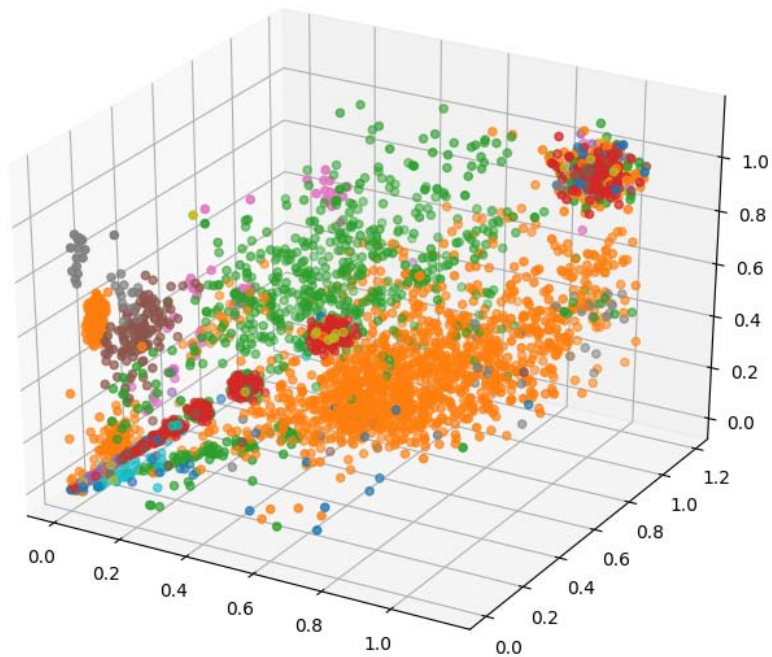
简单粗暴的规则无法满足“不影响业务”的要求，并能阻断绝大多数请求



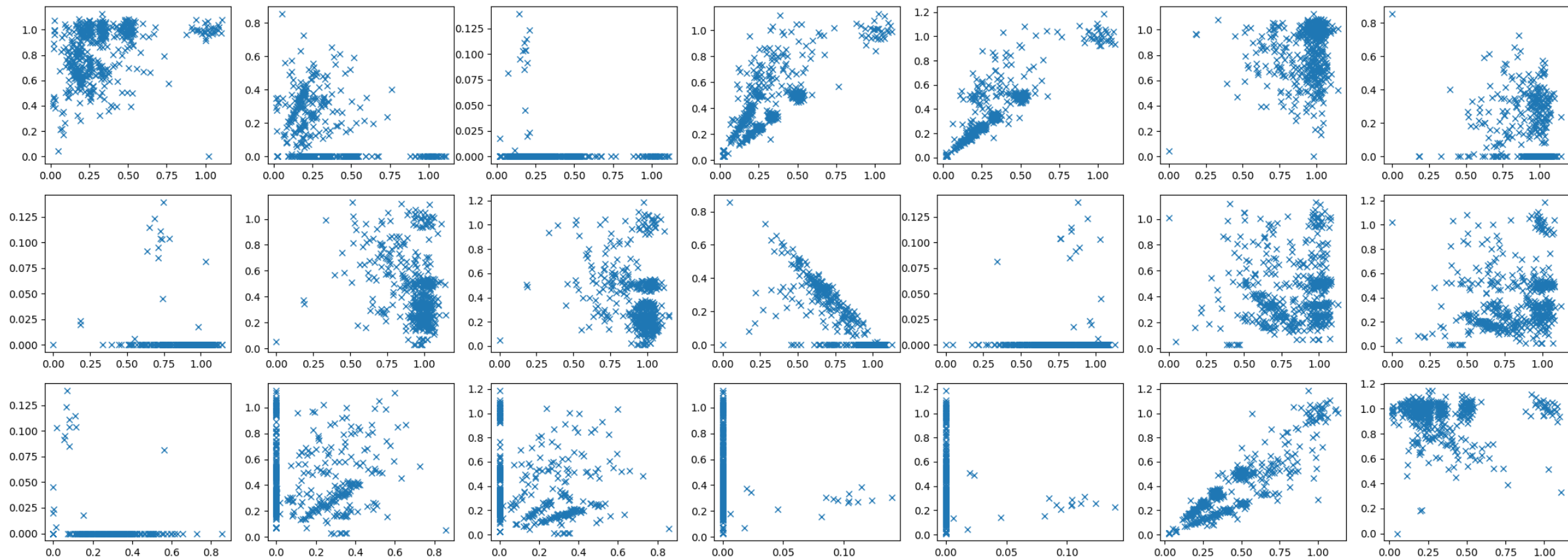
# 知所未知：高维数据超越人类感知能力

深度学习

可解决人类规则不可覆盖的细节问题

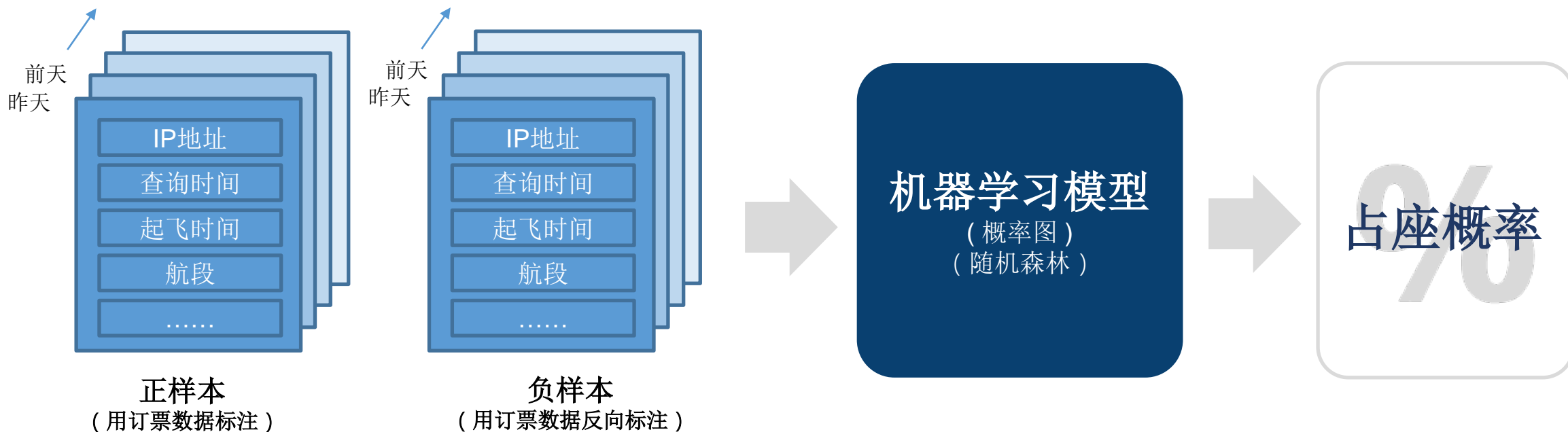


# 高维数据科学识别占座用户



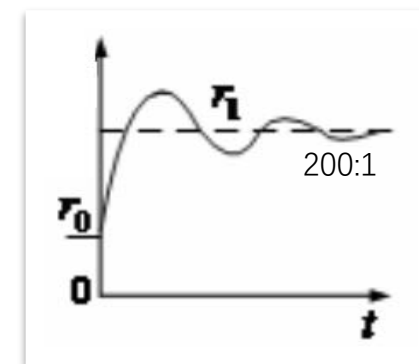
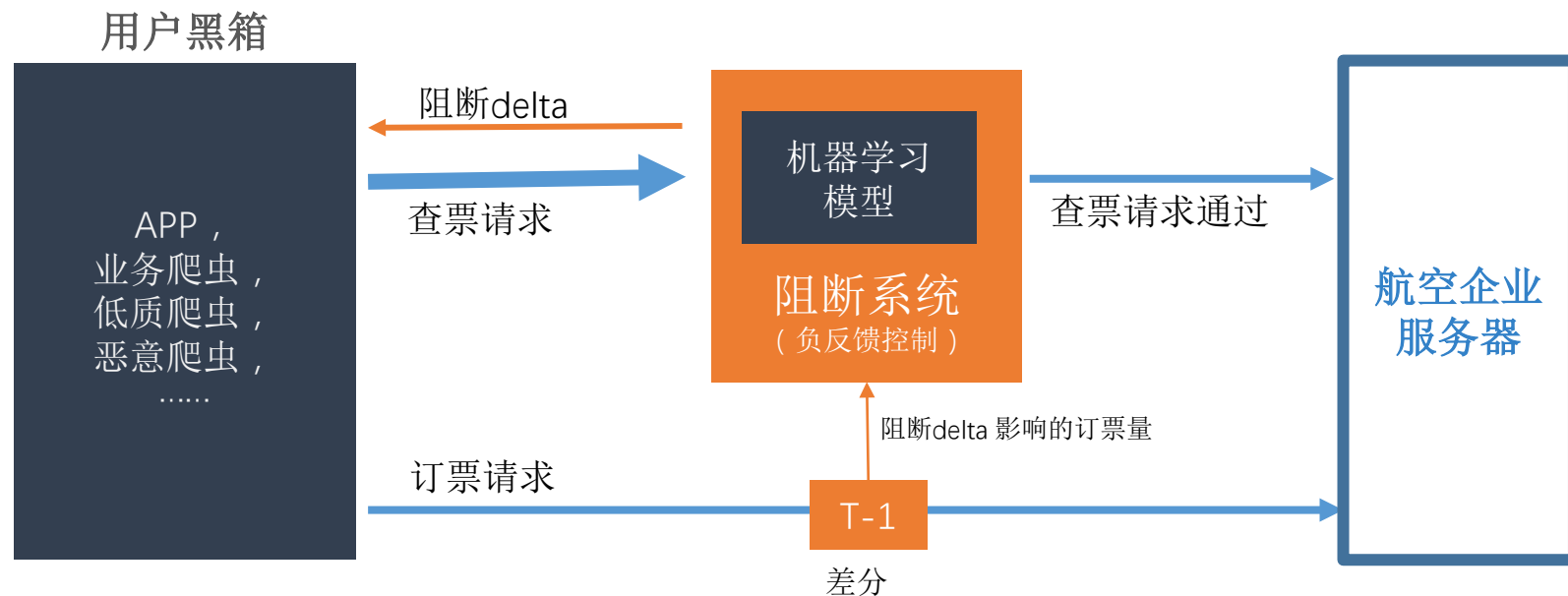
# 高维数据科学识别占座用户

**目标函数：** 订票数浮动允许范围内尽量多的减少退订比。  
**正样本：** 历史+昨天的订票支付数据。  
**负样本：** 历史+昨天的订票未支付数据。



## 基于负反馈的自动控制系统控制阻断：

- 渐进式学习：动态阻断方案，循序渐进阻断。
- 业务变更：在不影响数据维度的情况下，自动重新训练，适应业务变更
- 攻防：每天都会训练和自动学习前一天的订票影响情况，自动调整封杀策略。



自动控制过程

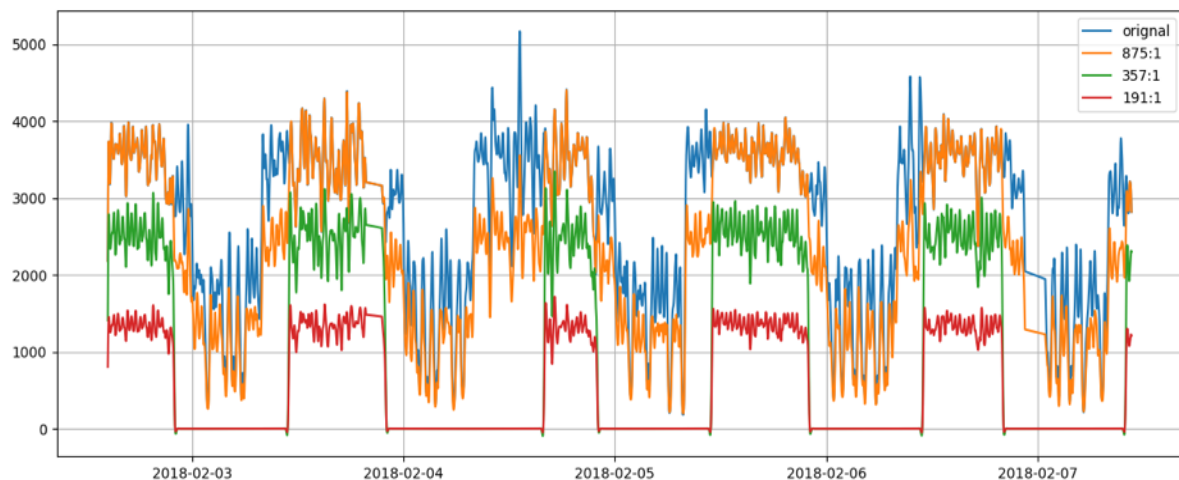
经过循序渐进的调整，查订比的优化会经历如下里程碑

**1025 : 1** → **875 : 1** → **357 : 1** →

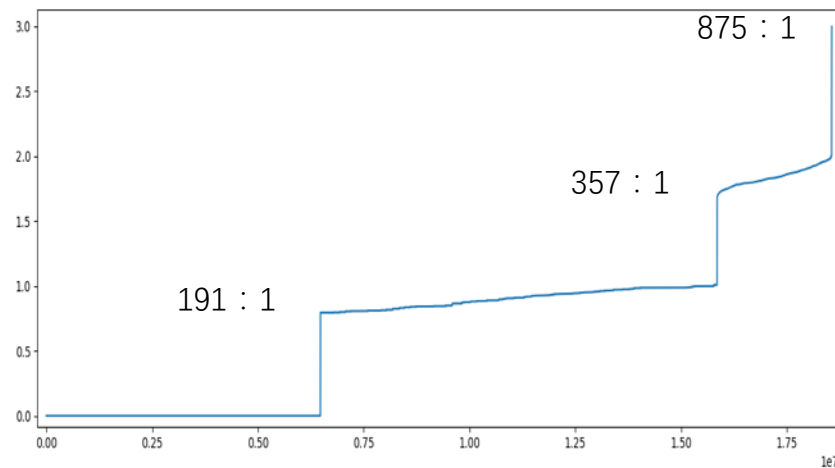
Original Milestone 1 Milestone 2

**191 : 1**

Milestone 3



不同阶段的过滤效果



不同里程碑对应的参数调整



# 人工智能对比传统规则在业务安全上的优势

传统业务安全技术
人工持续调整规则，反复攻防
机械阻断威胁
直接部署，定制开发
业务变更，升级软件
传统攻防识别

AI业务安全技术
负反馈机器学习模型，自动调整策略
结合业务，满足业务需求
针对场景，训练模型
如需要，根据数据训练模型
高维数据，深入业务聚类



VS





# 欢迎到梆梆安全的 展台沟通指导!

