阿里巴巴在线技术峰会
Alibaba Online Technology Summit

阿里聚安全在互联网业务中的创新实践

阿里巴巴 方超

Alibaba Group 阿里巴巴集团　阿里云 aliyun.com

安全环境的演变

安全环境演变趋势

互联网业务中的常见问题

2015年漏洞增长迅猛

系统漏洞：

2015年

iOS漏洞增长 1.28倍

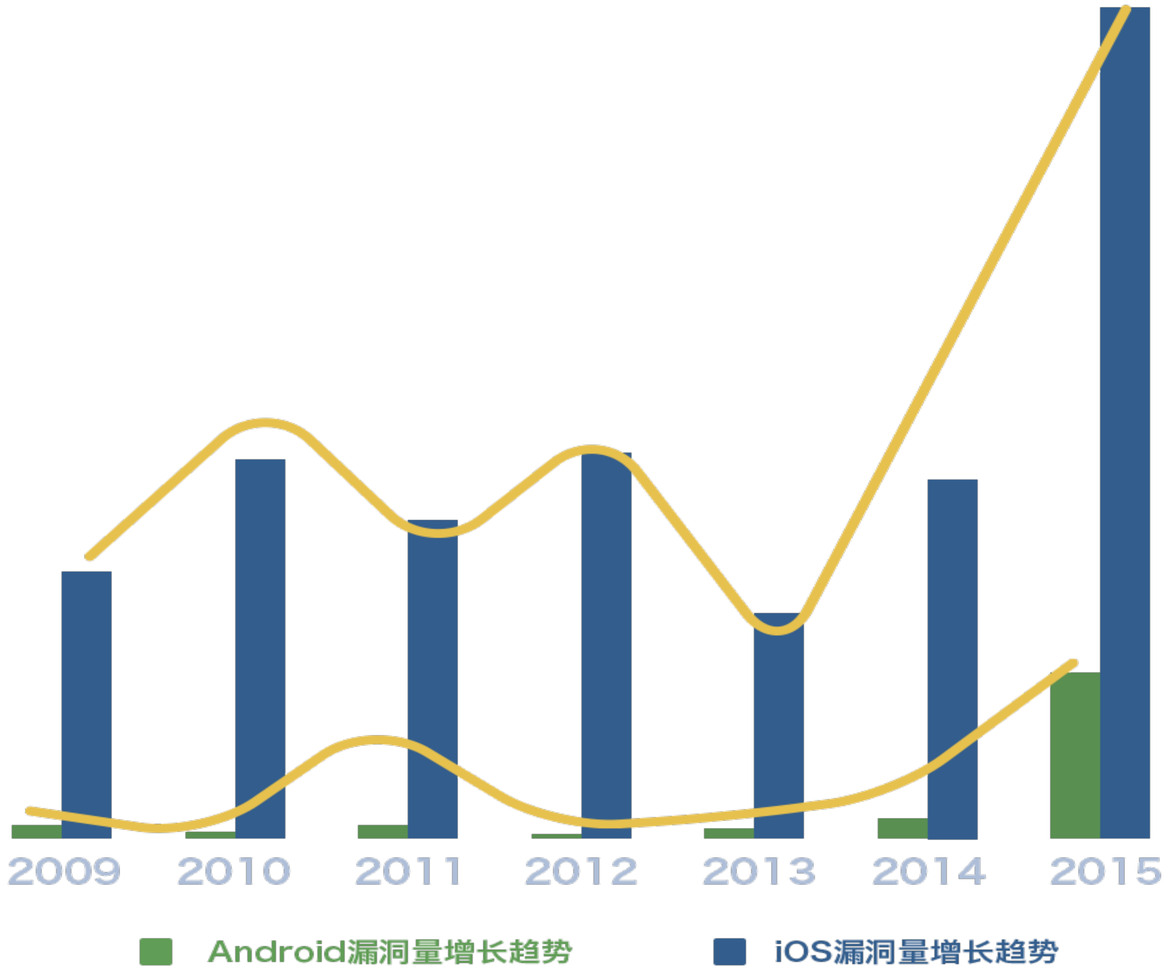
Android增长 10倍

应用漏洞：

18个行业TOP10的应用

97%的应用包含漏洞

平均每个应用有87个漏洞



移动端漏洞危害巨大

层出不穷的移动端APP漏洞

2016-05-22	远程命令执行
2016-05-21	计缺陷导致远程命令执行
2016-05-20	动修复fuzz服务端漏洞
2016-05-20	IP一句话木马
2016-05-20	远程代码执行
2016-05-19	ne端用户名密码抓取
2016-05-17	法存在安全问题
2016-05-16	下APP客户端某处存在SQL注入漏洞
2016-05-13	新版本绕过服务器的签名校验成功重打包
2016-05-13	盾的签名校验SDK逆向分析程序
2016-05-12	法存在安全问题
2016-05-11	库sign算法破解/详细过程
2016-05-11	安全问题
2016-05-11	机构钱包APP存在远程代码执行等多处安全隐患
2016-05-11	注入另外方式bypass（apache）
2016-05-09	网站逻辑缺陷导致可重置任意用户密码及短信轰炸
2016-05-09	器SOP绕过漏洞

系统级通用提权漏洞

CVE-2013-6282

CVE-2014-3153

CVE-2015-3636

CVE-2015-1805

互联网业务安全形势严峻

全网已泄漏个人账号超过21亿条
覆盖全网账号的40%以上

某P2P金融系统
日均垃圾账号申请量超过申请总量的50%

某O2O平台
2015年单次活动，现金券被刷最高达到70%

安全的挑战 - 互联网业务复杂

业务种类多

风险多变

海量风险事件

安全的挑战 - 防控链路长

业务链路长分支多

涉及人员节点多

控制能力弱

安全的挑战 - 涉及技术面广

平台种类多

技术种类多

攻防要求高

互联网业务的层次

	手淘	视频应用
内容	商品图片和信息	视频、互动评论
用户	买家、卖家	普通用户、会员、主播
服务	购买、促销、秒杀、抽奖	视频与直播服务
应用	电商 APP	直播 APP
数据	交易数据	内容数据
传输	移动网络	移动网络
系统	操作系统	操作系统
硬件	手机	手机

围绕业务的安全模型

违禁内容	涉黄图片		L 8	智能鉴黄	文本过滤	违禁识别	图文识别
垃圾账户	虚假身份		L 7	身份造假识别	身份冒用识别		
黄牛刷单	活动作弊	账号盗用	L 6	风险识别	安全验证		
逻辑逆向	破解外挂	应用漏洞	L 5	漏洞扫描	应用加固	仿冒监测	
数据窃取	数据伪造		L 4	数据防爬	安全存储		
信息截取	消息伪造	流量劫持	L 3	安全加密	安全签名		
系统漏洞	病毒木马		L 2	木马查杀			
硬件漏洞	协议漏洞		L 1	物联网风险检测			

8层安全模型

阿里聚安全 - 聚焦互联网业务安全

传统IT业务

封闭的环境
有限的账号
可控的终端

互联网业务

开放的环境
海量的账号
不可控的终端

以系统为中心的安全

通过保护主机、网络、终端来构建安全体系

以业务为中心的安全

围绕业务来构建安全体系

业务的支撑者

业务的不可分割部分

阿里聚安全 - 移动安全

移动互联网时代下的安全基石

检测

木马扫描
- 快速检测恶意代码、广告插件
- 外包APP安全性检测
- 第三方SDK代码安全性检测

漏洞扫描
- 技术漏洞发现率>95%
- 提升应用自身安全风险
- 提供基于实战的分级机制与修复建议

安全评估服务
- 业界顶尖安全专家团队评估
- 深度渗透移动应用及相关业务，发掘安全隐患
- 提供应用全生命周期改进建议

防护

安全组件
- 快速组件化接入
- 业界独创的端安全能力
- 亿级应用久经攻防考验

应用加固
- 提供了快速加固，多渠道加固以及自定义加固，对抗各类分析工具
- 实战验证高兼容性、高稳定性、高性能
- 深度混淆技术对抗实际风险

专家服务
服务端API
移动端SDK
网站 jaq.alibaba.com

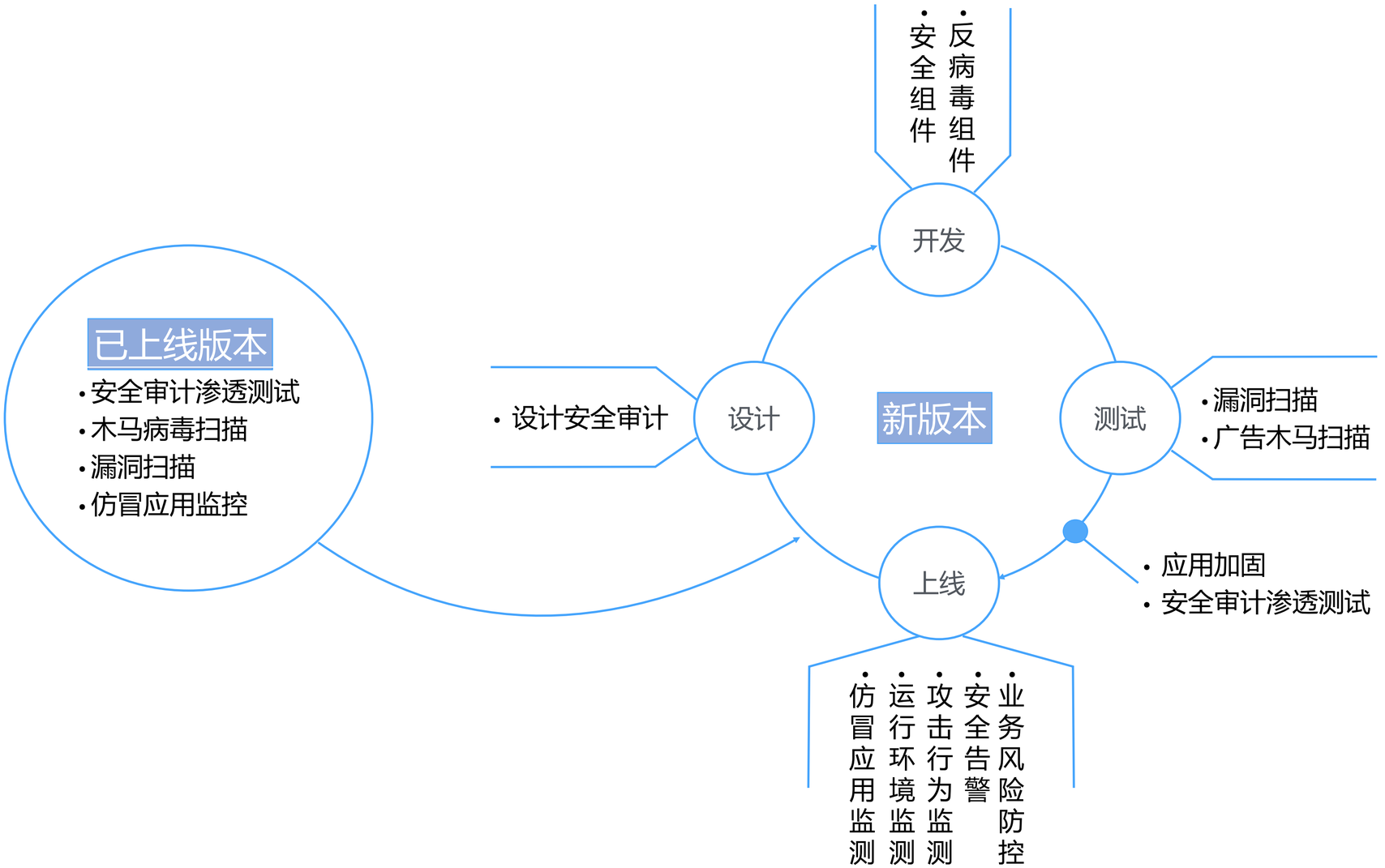
监控

安全告警
- 业界漏洞、安全风险第一时间通报
- 规避或解决方案的建议

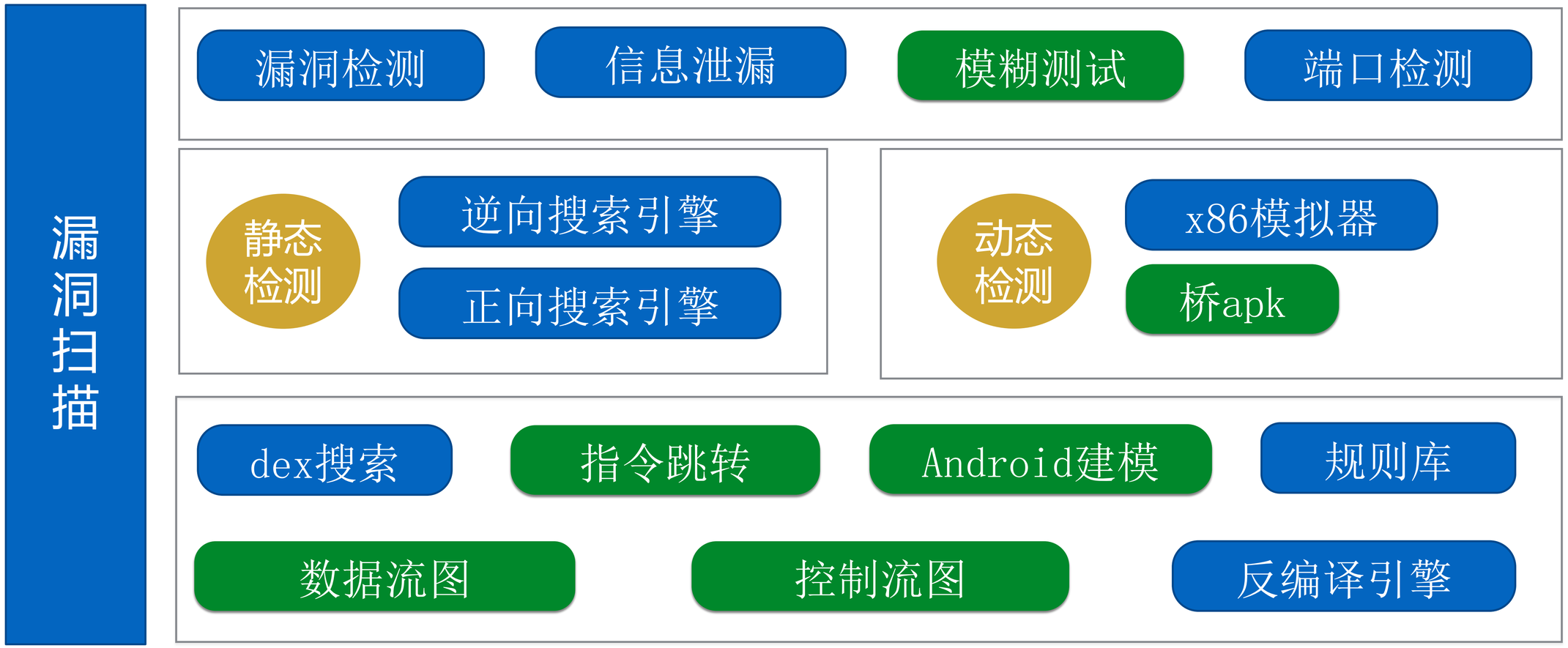
仿冒监测
- 大数据监测全网活跃应用,论坛，网盘等高风险渠道
- 伪基站钓鱼监测
- 多维度仿冒检测能力

应用风险感知
- 依托安全组件实现实时风险发现
- 运行环境监测（Root / 模拟器）
- 攻击行为监测（注入 / 篡改 / 调试）
- 配合数据风控进行业务防控

阿里聚安全 - 移动APP全流程防护



阿里聚安全 - 移动端漏洞扫描



阿里聚安全 - 移动端应用加固

Only Apk Protection?

体积

兼容性

稳定性

应用加固

Java 保护

- 指令翻译
- 全量混淆
- 常量加密
- 函数虚拟化保护

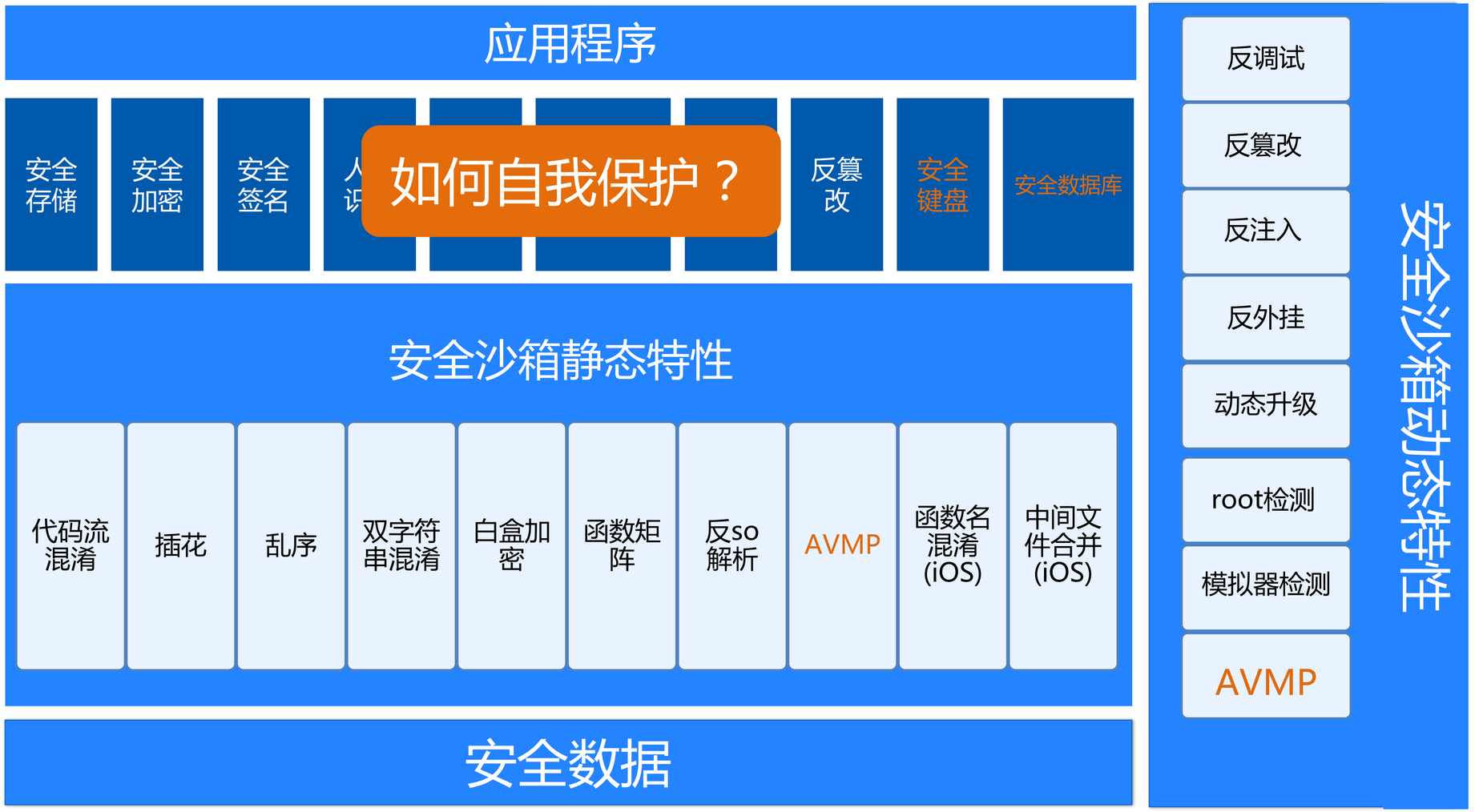
So 保护

- So加壳动态保护
- 加入花指令
- 自定义elf保护格式

Apk 保护

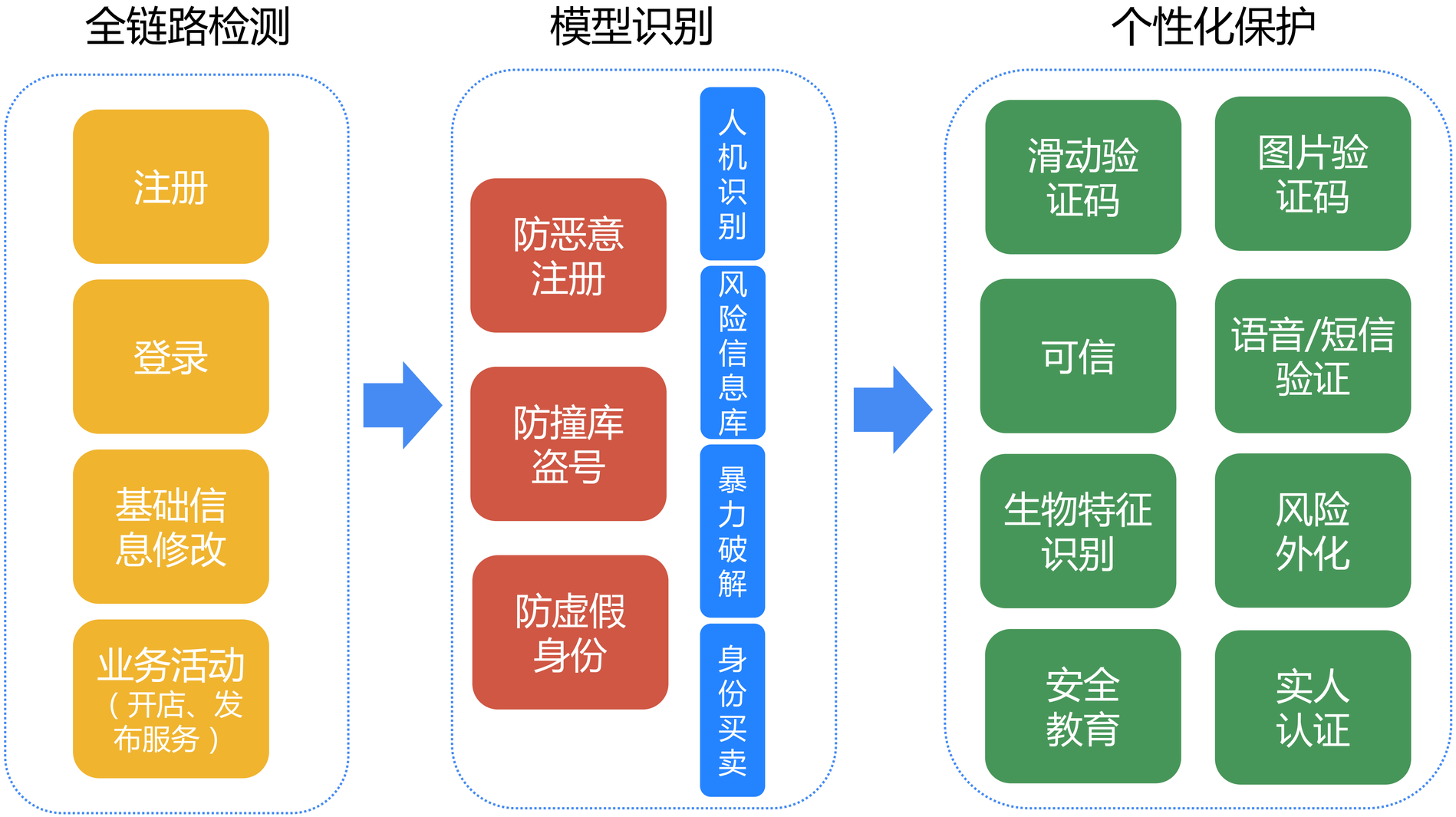
- Dex内存分散存储
- Apk代码整体加密
- 资源保护
- 反内存dump
- 反二次打包
- 反各种静态分析工具

阿里聚安全 - 移动端安全组件

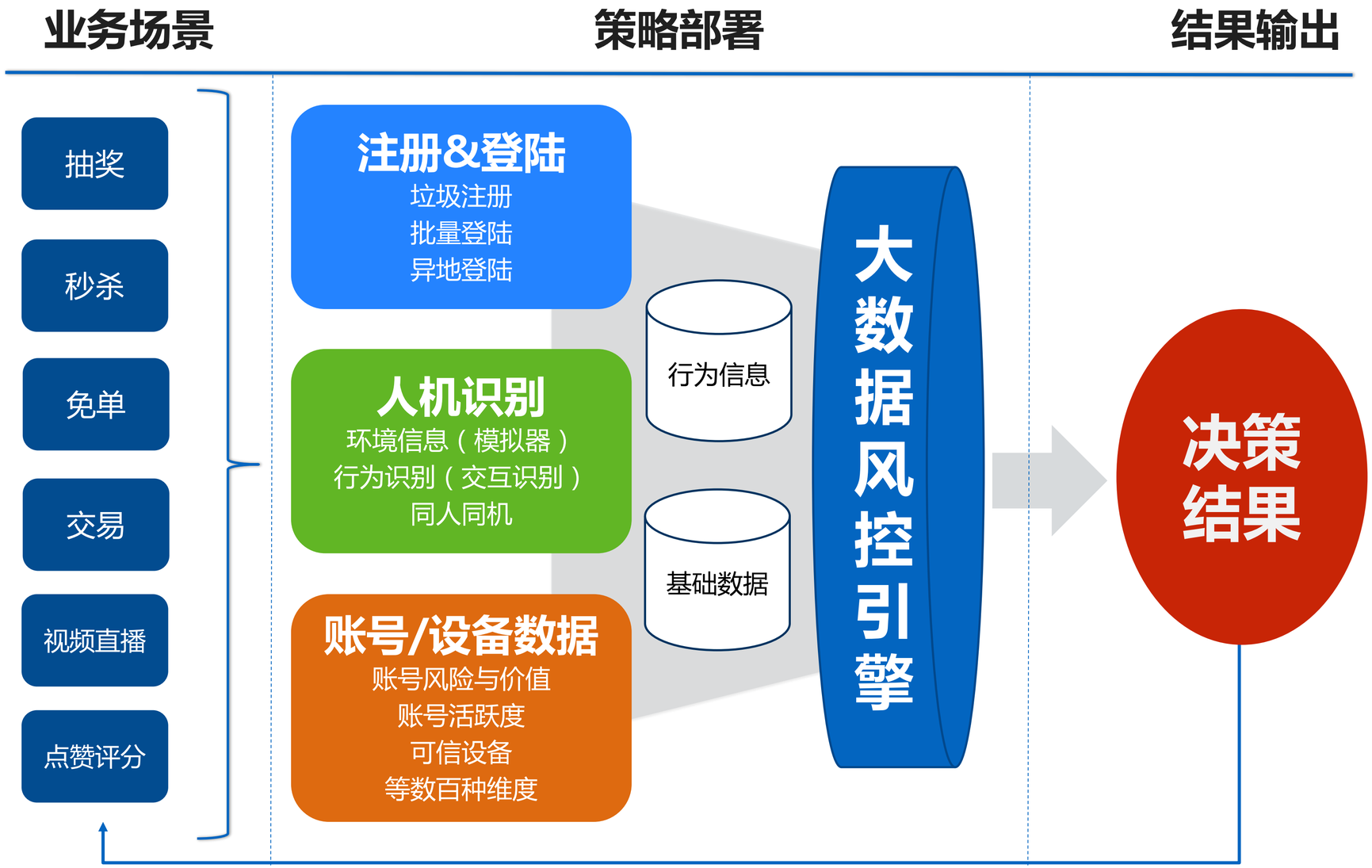


利用安全组件的各项技术一站式解决数据安全、机器识别、逆向对抗、设备指纹等多种问题

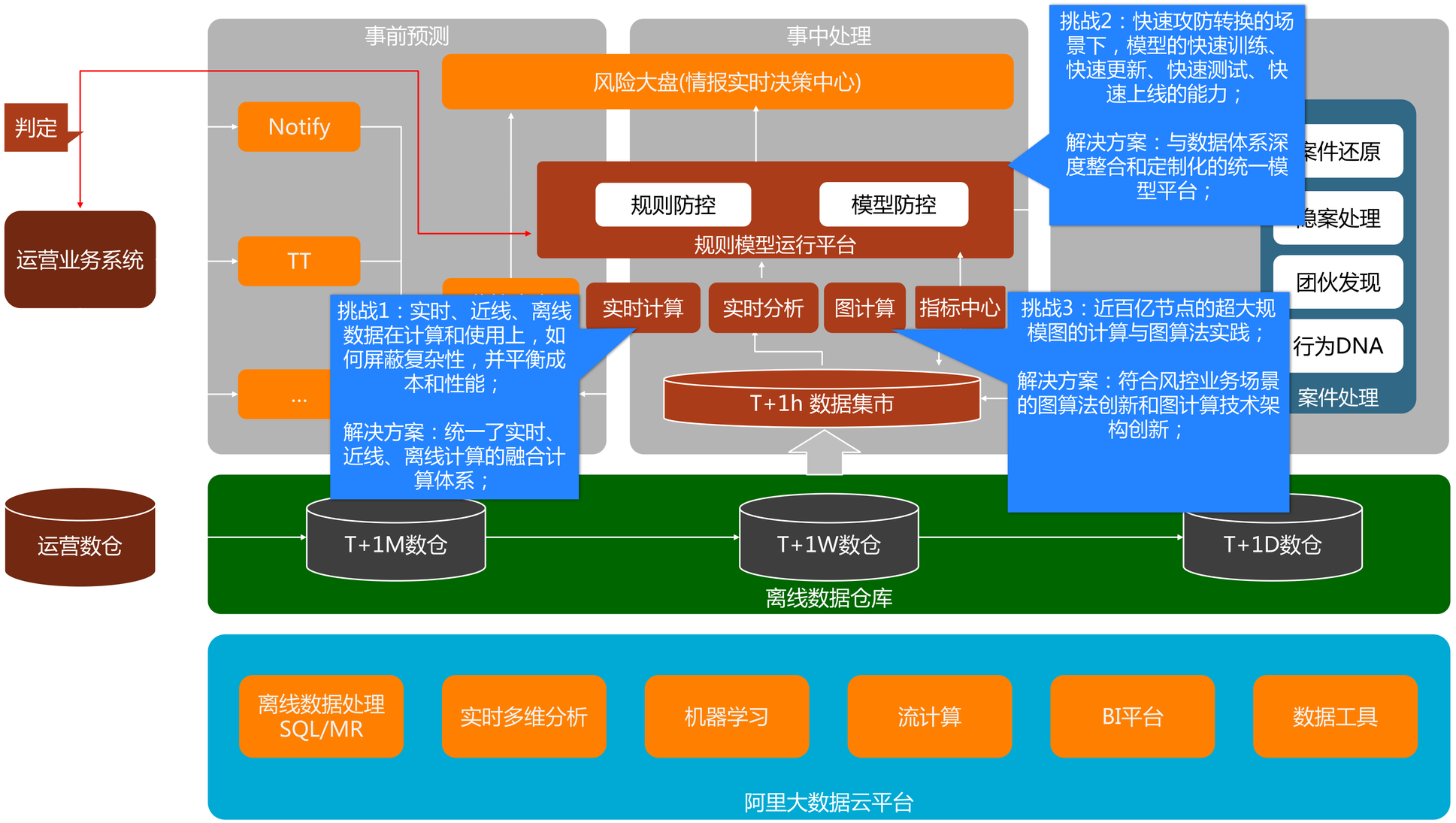
阿里聚安全 - 数据风控（帐号安全）



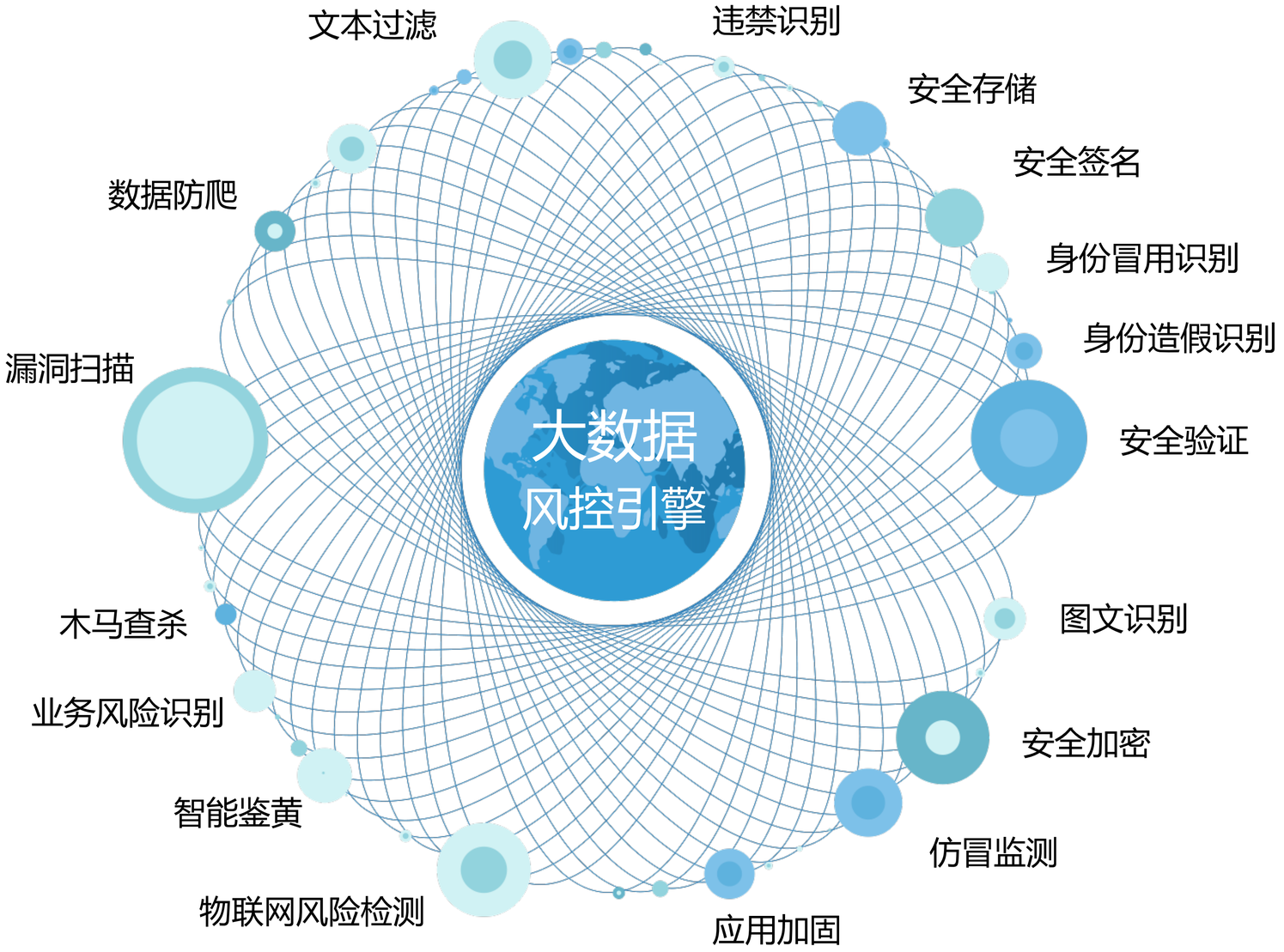
阿里聚安全 - 数据风控


业务场景
策略部署
结果输出
抽奖
秒杀
免单
交易
视频直播
点赞评分
注册&登陆
垃圾注册
批量登陆
异地登陆
人机识别
环境信息（模拟器）
行为识别（交互识别）
同人同机
账号/设备数据
账号风险与价值
账号活跃度
可信设备
等数百种维度
行为信息
基础数据
大数据风控引擎
决策结果

阿里聚安全 - 基于多层数据处理技术的体系



阿里聚安全 - 全链路防控体系



阿里聚安全