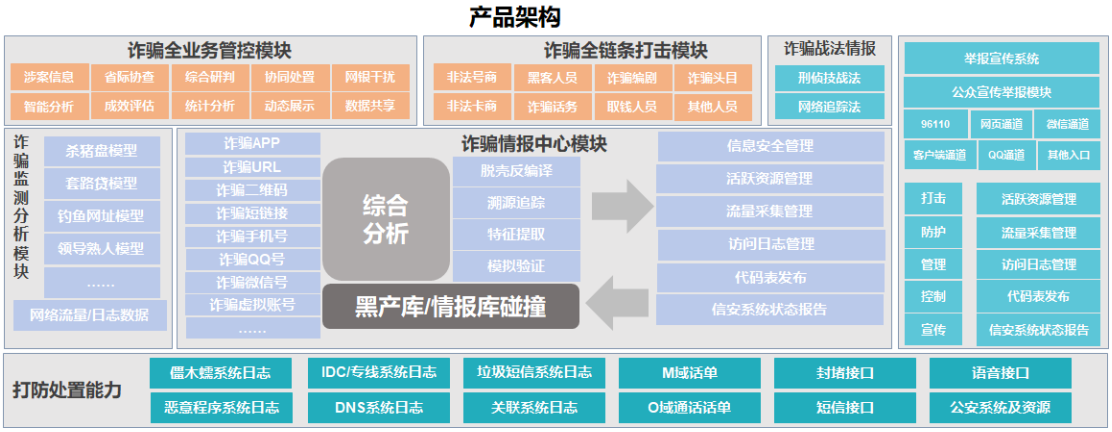
互联网反诈管控平台

1、产品简介

互联网反诈管控平台基于多维度数据采集、分析、规则匹配、拦截手段为用户提供高效，安全的上网安全防护服务，针对传统电信与新型互联网诈骗场景，面向运营商、公安、监管等客户，依托反诈规则库、用户上网行为监测、拦截、涉诈事件预警等功能，高效过滤通过伪基站、即时通信、邮件、网页弹窗等多种方式传播互联网欺诈行为。

2、产品架构



3、核心功能

- **APP反诈分析：**

（1）支持下载源过滤：当apk从安全可信的网站下载时，可认为软件为非诈骗软件；对于下载源不在白名单中的应用，会还原文件并进行静、动态检测。

（2）支持静态检测：支持根据特征进行情报库匹配、反编译检测。

（3）支持动态检测：根据侦测的样本数据进行人工智能分析，输出分析结果，检测恶意 app。

（4）支持 apk 逆向分析：支持逆向提取应用名称和包名。

- **网址反诈分析：**

收集并记录了已知的涉及欺诈、钓鱼、赌博、色情传播等不良行为的网址信息，形成涉诈网址库并进行分类和分级。

通过对已发生网址涉诈犯罪案件进行 IP 侦测、反查侦测、语义分析、网页指纹分析、图形分割分析等手段对多个不同维度信息综合关联分析建模，形成针对网址诈骗的诈骗模型库，包括：婚恋交友（杀猪盘）、返利（刷单、游戏）、虚拟投资理财、虚拟网络贷款、博

彩色情、医疗代孕、仿冒政务公检法等，并通过不断研究新发案件，对模版库迭代更新。

- **行为分析**

通过深入剖析真实诈骗案例，提取相关涉诈特征，以诈骗人和受害者视角建立了多种检测模型。通过将采集设备上报的话单数据进行用户行为关联，并与模型进行匹配碰撞，能够高效识别出涉诈行为。包括：FaceTime 涉诈分析、蝙蝠、mostalk 等密聊类应用分析、爱思远控、手机远程协助控制等远控行为分析、物卡人用、静默行为分析。

4、 产品价值与优势

- **精准的诈骗网址特征库**

（1）来源广：特征库情报来源于自主安全团队发现、互联网安全厂商、运营商、公安部、相关管理部门。

（2）准度高：统计特定区域用户经常访问的有害网址类型，经上报主管部门审核后，实施拦截封堵，从而更精准的对用户进行拦截提醒。

（3）时效强：搜集每日全球新增域名并实时进行研判，全球每日新增域名 30W-40W，日均研判能力 300W-400W。

- **情报数据的持续演进**

（1）案件情报：从诈骗案件中提取反诈情报，自动化、流程化监测和预警

（2）12321 投诉情报：从投诉信息中挖掘反诈情报，优化诈骗检出准确率

（3）举报情报：从举报平台获取诈骗情报，实现从 1%~99%的跨越

（4）取证情报：从取证平台中获取情报数据，作为诈骗检出的磨刀石

（5）扩线情报：从多维渠道对诈骗情报进行关联扩线，不断扩大情报深度和广度

（6）挖掘情报：对涉诈线索进行挖掘，进一步获得诈骗人和团伙的情报信息，为打击、治理提供基础