AVL移动安全·安天

APP 用户权益保障合规检测方案

安天移动安全
www.avlsec.com

目录

第 1 章　前言

1.1 个人信息保护成为移动网民的关注焦点

截止 2020 年 12 月，我国网民规模达到 9.89 亿，手机网民规模达到 9.86 亿，占比 99.7%，标志着中国已经全面进入移动互联网时代。伴随着移动端安全技术水平的不断革新，得益于中央及地方监管机构的关注和推动，移动终端用户的安全防护意识不断提升，安全能力服务商也主动承担起更多的社会责任，中国网民遭遇安全事件呈现下降趋势，总体向好发展。

然而与此同时，灰色产业链正凭借监管和安全防御的相对稀松之地大肆发展，冰山之下暗流涌动。其中，通过统计近半年用户关心事件的平台指数可以发现，个人隐私信息保护问题越发成为用户的安全关注焦点之一。

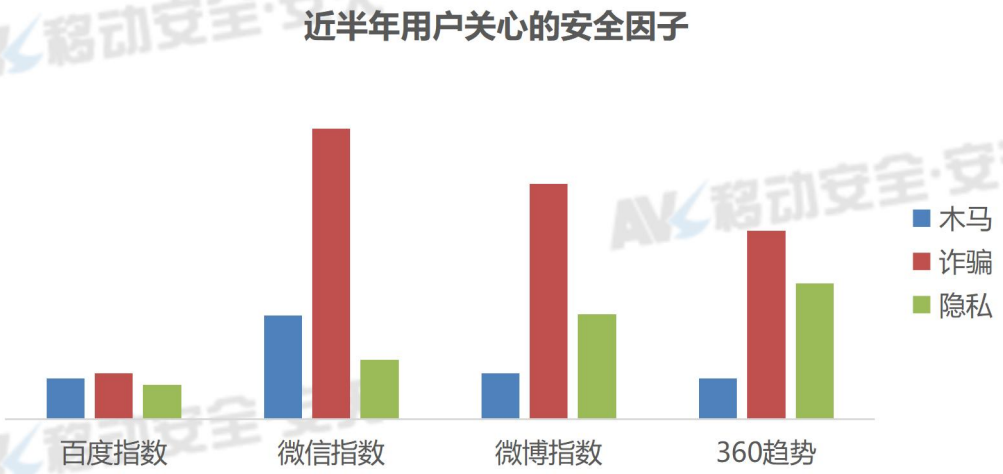

图 1.3：用户关心安全因子

1.2 公民隐私地下交易成为灰色产业链的主要催化剂

随着大数据产业的不断发展，数据商业化价值在越来越多的行业被广泛认同，用户个人信息成为了一项热门资源，从而逐渐催生出包含公民隐私在内的各类个人信息的肆意采集和地下交易灰产。

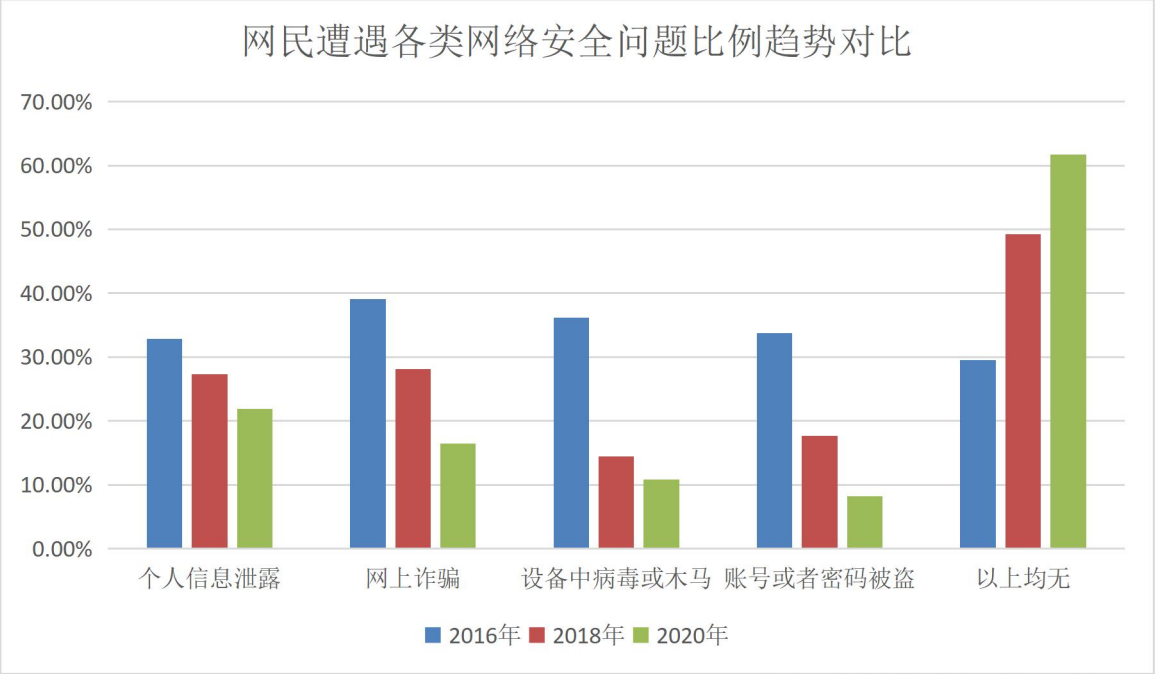

图 1.1：网络遭遇各类网络安全问题比例趋势对比

从图中可以看出，截止到 2020 年末，个人信息泄露这一网络安全问题日趋突出，成为了主要的网络安全问题。（数据来源：第 39 次、第 43 次、第 47 次|中国互联网络发展状况统计报告）

2019 年，工信部信通院持续从国内 top 应用商店中挑选社交通信、地图导航、网上购物等 20 个类别，下载量大影响广的 200 多款 App 作为检测对象进行合规性检测，共发现 1200 多项个人信息违规问题，其中 top5 的问题见下图。

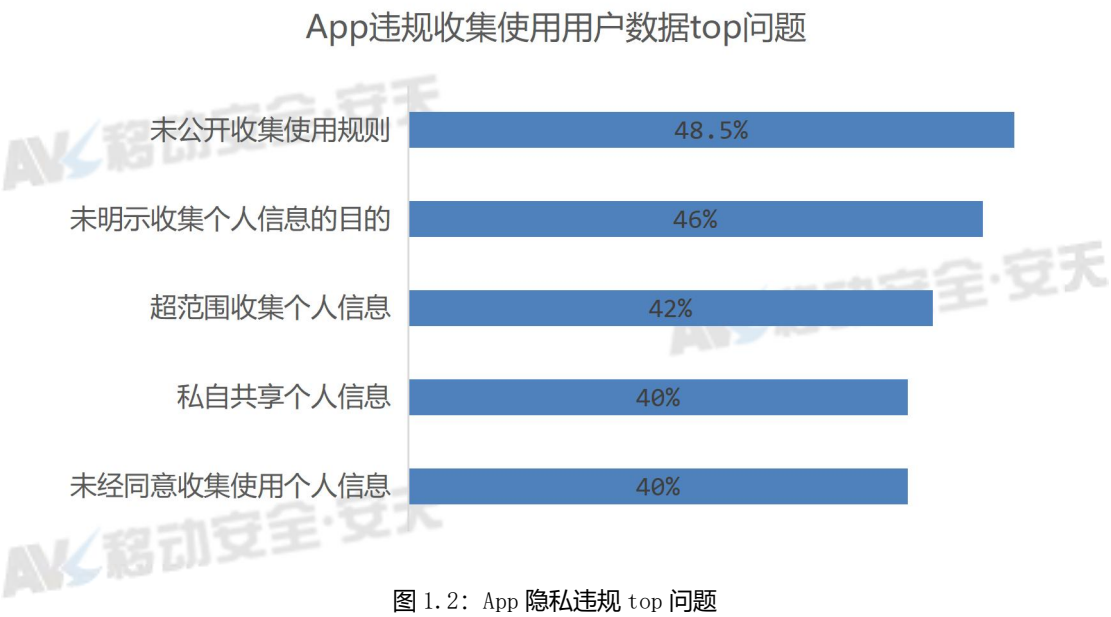

图 1.2：App 隐私违规 top 问题

1.3 监管重拳出手移动用户权益保护

2017 年 6 月 1 日《中华人民共和国网络安全法》正式实施，同年全国信息安全标准化技术委员会发布《信息安全技术个人呢信息安全规范》，并于 2018 年 5 月 1 日正式实施。2019 年 8 月，信安标委发布《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》，用户权益保护进入加速落实阶段。

2019 年 1 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展 APP 违法违规收集使用个人信息专项治理的公告》，开始在全国范围组织开展 APP 违法违规收集使用个人信息专项治理，成立了 APP 违法违规收集使用个人信息专项治理工作组。随后印发了《App 违法违规收集使用个人信息行为认定方法》（以下简称《认定方法》），并基于此由工业和信息化部先后下发《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知（工信部信管函〔2019〕337 号）》、《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知（工信部信管函〔2020〕164 号）》。

第 2 章　方案介绍

2.1 方案概述

APP 用户权益保障合规检测方案结合安天多年来对于恶意软件、风险软件以及应用不规范行为的识别、分析、评估和判定的经验积累，融合自然语言处理和机器学习等技术手段，通过对 APP 隐私政策和应用行为的识别来实现对 APP 侵害用户权益行为检测能力的技术方案。

检测服务系统总体采用 SaaS 服务形态，通过云端接口投放并回调检测结果。整体服务包含隐私政策判定和语义分析服务、静态检测服务、动态沙箱检测服务等多个业务模块，通过集群化部署和管理对投放任务可进行高效的检测。

图 2.1：用户权益保障合规检测技术架构图

2.2 业务流程说明

APP 用户权益保障合规检测方案主要包括两个业务单元，即后端业务流转单元和终端检测单元。

后端业务流转单元承载任务任务调度、样本下载、隐私政策文件爬取、隐私政策判定、隐私政策语义分析、样本静态检测、终端任务下发、结果判定及封装、结果回调等工作。

终端检测单元承载检测项的逻辑实现，模拟用户使用场景，完成应用的安装、运行、遍历、行为触发、证据采集、应用卸载等相关操作。

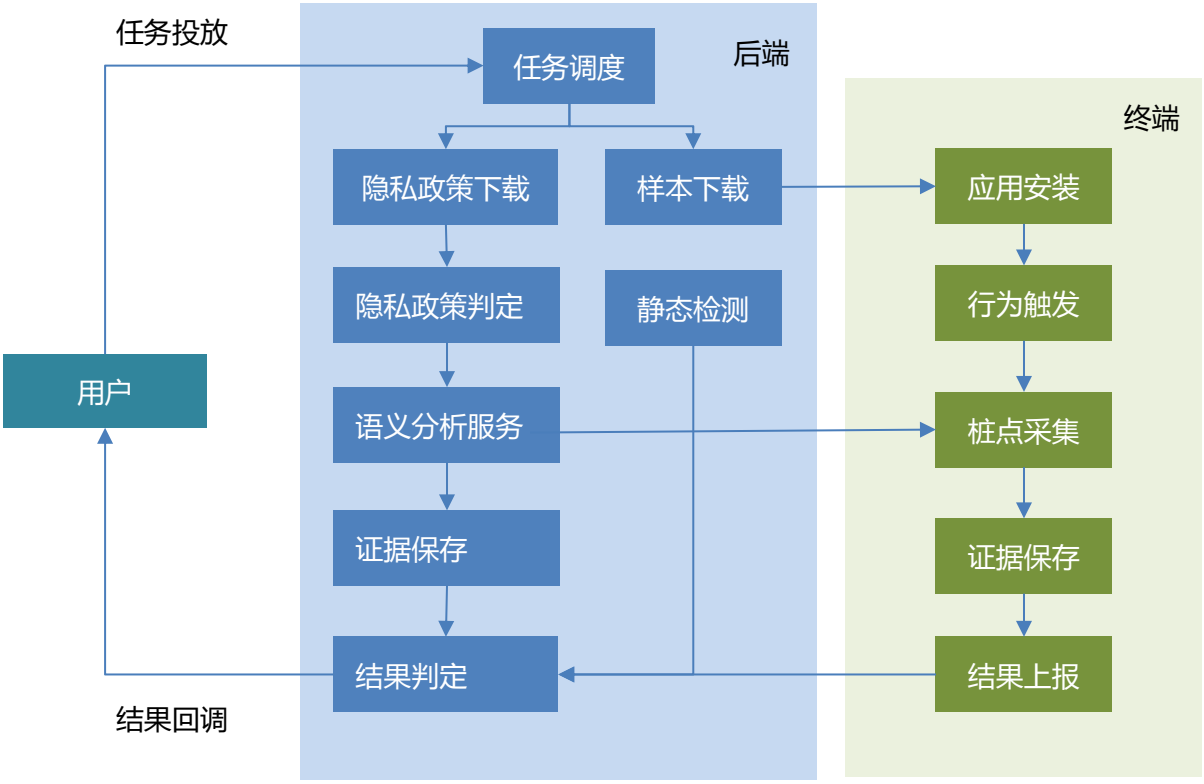

图 2.2：APP 用户权益保障合规检测系统流程图

2.3 检测项说明

安天 APP 用户权益保障合规检测方案通过近年来总结归纳的常见违规收集用户个人信息行为，结合政策文件的深入解读并凭借安天丰富的移动应用威胁治理经验、成熟的沙箱化安全检测自研技术以及运营能力，面向合作伙伴开放全面的用户权益保障合规检测能力，其中超过一半的检测项获得主管部门认可与应用，为合作伙伴提供一站式的移动应用用户权益保障合规检测服务。具体包括如下检测项：

表 2.1：用户权益保障合规检测项一览表

case_number	type_name	rule_title	rule_number	rule_content	case_desc
1	APP、SDK 违规处理用户个人信息方面	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）	1.1	违规收集个人信息。重点整治 APP、SDK 未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。	APP 未见向用户明示个人信息收集使用的目的、 方式和范围， 未经用户同意， 存在收集 IMEI、 设备 MAC 地址和软件安装列表、通讯录和短信的行为。
2					APP 以隐私政策弹窗的形式向用户明示收集使用规则， 未经用户同意， 存在收集 IMEI、 设备 MAC 地址和软件安装列表、 通讯录和短信的行为。
3					APP 以隐私政策弹窗的形式向用户明示收集使用规则， 但未见清晰明示 APP 收集设备 MAC 地址、 软件安装列表等的目的方式范围， 用户同意隐私政策后， 存在收集设备 MAC 地址、 软件安装列表的行为。
4					APP 未见向用户明示 SDK 收集使用个人信息的目的、方式和范围， 未经用户同意， SDK 存在收集 IMEI、 设备 MAC 地址和软件安装列表、 通讯录和短信的行为
5					APP 向用户明示 SDK 的收集使用规则， 未经用户同意， SDK 存在收集 IMEI、 设备 MAC 地址和软件安装列表、 通讯录和短信的行为。
6					APP 向用户明示 SDK 的收集使用规则， 但未见清晰明示 SDK 收集设备 MAC 地址、软件安装列表等的目的方式范围， 用户同意隐私政策后， SDK 存在收集设备 MAC 地址、 软件安装列表的行为。
7					App 在征求用户同意环节， 未提供明确的同意或拒绝按钮， 或者使用 “ 好的” “ 我知道了” 等词语。
8					App 在征求用户同意环节， 设置为默认勾选。
9			1.2	超范围收集个人信息。重点整治 APP、SDK 非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集	APP 在运行时， 未见向用户告知且未经用户同意， 存在每 30s 读取一次位置信息，非服务所必需且无合理应用场景， 超出实现 产品或服务的业务功能所必需的最低频率。
10					APP 未见向用户明示 SDK 的收集使用规则，未经用户同意， SDK 存在每 30s 读取一次位置信息， 非服务所必需且无合理应用场景， 超出实现产品或服务的业务功能所必需的最低频率。

11				个人信息的行为。	APP 未见向用户告知且未经用户同意， 在静默状态下或在后台运行时， 存在收集通讯录、 短信、 通话记录、 相机等信息的行为，非服务所必需且无合理应用场景， 超出与收集个人信息时所声称的目的具有直接或合理关联的范围。
12					APP 未见向用户告知且未经用户同意， 在静默状态下或在后台运行时， 存在按照一定频次收集位置信息、 IMEI、 通讯录、 短信、图片等信息的行为， 非服务所必需且无合理应用场景， 超出与收集个人信息时所声称的目的具有直接或合理关联的范围。
13					APP 未向用户明示 SDK 的收集使用规则，未经用户同意， SDK 在静默状态下或在后台运行时，存在收集通讯录、 短信、 通话记录、 相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。
14					APP 未向用户明示 SDK 的收集使用规则，未经用户同意， SDK 在静默状态下或在后台运行时，存在按照一定频次收集位置信息、 IMEI、 通讯录、 短信、 图片等信息的行为， 非服务所必需且无合理应用场景， 超出与收集个人信息时所声称的目的具有直接或合理关联的范围。
15			1.4	强制用户使用定向推送功能。重点整治 APP、SDK 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。	APP 的 YYY 页面或功能存在定向推送功能，但隐私政策未见向用户告知， 将收集的用户个人信息用于定向推送、 精准营销。
16	设置障碍、频繁骚扰用户方面		2.5	APP 强制、频繁、过度索取权限。重点整治 APP 安装、运行和使用	APP 首次启动时， 向用户索取电话、 通讯录、定位、 短信、 录音、 相机、 存储、 日历 等权限， 用户拒绝授权后， 应用退出或关闭（ 应用陷入弹窗循环， 无法正常使用） 。

17				相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。重点整治短时长、高频次，在用户明确拒绝权限申请后,频繁弹窗、反复申请与当前服务场景无关权限的行为。重点整治未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。	用户注册登录时， APP 向用户索取电话/通讯录/定位/短信/录音/相机/存储/日历等权限， 用户拒绝授权后， 应用无法正常注册或登录。
18					APP 在用户明确拒绝通讯录/定位/短信/录音/相机/XXX 等权限申请后， 重新运行时，仍向用户弹窗申请开启与当前服务场景无关的权限， 影响用户正常使用。
19					APP 首次打开（ 或其他时机） ， 未见使用权限对应的相关产品或服务时， 提前向用户弹窗申请开启通讯录/定位/短信/录音/相机/XXX 等权限。
20			2.6	APP 频繁自启动和关联启动。重点整治 APP 未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方 APP 的行为。	APP 非服务所必需或无合理应用场景， 超范围频繁自启动或关联启动第三方 APP。
21	欺骗误导用户方面		3.7	欺骗误导用户下载 APP。重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，特别是具有分发功能的移动应用程序欺骗误导用户下载非用户所自愿下载 APP 的行为。	XXXXX 广告页面/开屏广告/主屏/功能,无显著 APP 下载提示，点击即自动下载非用户所自愿下载 APP。 XXXXX 广告页面/开屏广告/主屏/功能，以“是否立即开始游戏”方式欺骗误导用户自动下载非用户所自愿下载 APP。 XXXXX 广告页面/开屏广告/主屏/功能，以“领取红包”方式欺骗误导用户自动下载非用户所自愿下载 APP。 XXXXX 广告页面/开屏广告/主屏/功能，点击“下载按钮“以外区域，自动下载非用户所自愿下载 APP。

22					APP 中信息窗口（开屏页广告等），未见存在关闭或退出窗口的标识。
23					APP 中信息窗口（开屏页广告等），存在虚假无效的关闭或退出窗口标识。
24					APP 中信息窗口（开屏页广告等），无显著提示，点击页面任意位置即跳转至第三方应用或拉起第三方广告页面。
25	其他		其他	其他	App 存在拦截用户按键消息,进行信息窗口推送的行为。
26					App 在用户解锁终端后,从后台弹出信息窗口的行为。 App 在后台状态下，弹出广告弹窗的行为。 App 在其他 App 应用上方，弹出广告弹窗的行为。
27					App 在后台状态下，弹出信息窗口的行为。

第 3 章　产品优势与价值

3.1 产品优势

3.1.1 成熟的沙箱检测技术

由于 Android 系统的频繁升级和底层权限的逐步收紧，对于自动化检测方案的适配和拓展提出了很高的要求，尤其是基于安全对抗日趋严重的大环境下，部分应用对沙箱环境有了一定的识别和对抗能力，因此成熟的真机模拟沙箱检测技术就显得尤为关键。

安天早在 2015 年就开始自研沙箱检测技术，在真机部署仿真沙箱运行模拟环境拥有成熟的技术架构和研发体系。对于真机集群的系统适配、桩点预埋、任务调度等方面积累了丰富的经验，重点体现在：

- 集群化的系统适配、部署和调试
- 已基于 ASOP 适配了不同 Android 系统的版本，能快速部署上线
- 成熟的工程化业务流转流程，采用独立的功能模块，可支持产品敏捷迭代

在安天自研的真机沙箱环境中，通过 Hook 技术实现对系统核心进程的监控，从而可以实现系统层核心 API 的 Hook 以及底层行为数据的获取。通过对核心进程的控制，能确保框架具有良好的适配性和可扩展性，从而能规避系统升级导致的不兼容风险。

通过在真机沙箱环境中通过预置污点数据，对系统设置、预装应用、网络环境等多个维度进行了模拟用户真实场景的配置，保证应用违规收集用户数据的行为能充分的激发暴露。

在应用遍历和行为触发场景方面，安天设计了一套应用功能和 UI 界面遍历方案，通过机器学习技术分析应用界面元素和控件，有策略的进行拟人化交互操作，最终快速高效的完成应用功能和界面的遍历。

3.1.2 基于深度学习的判定

用户权益保障的主体对象实际是用户个人信息，而应用对于用户个人信息的收集使用是通过隐私政策声明来体现告知义务并获得授权许可的。所以隐私政策的识别和判定对于用户权益保障至关重要。

为了建设语义分析能力，安天通过多年来建立的顶级应用安全检测运营体系，获取了海量的应用样本和隐私政策文本。通过分析团队人工以及自动化持续打标，筛选了大量可供学习的隐私政策范本。再由算法工程师设计研发语言处理模型，并对海量隐私政策进行智能学习，形成了隐私政策内容合规的检测范式标准，并在检测过程中通过不断的机器学习对隐私政策声明内容是否合规进行深度判定。

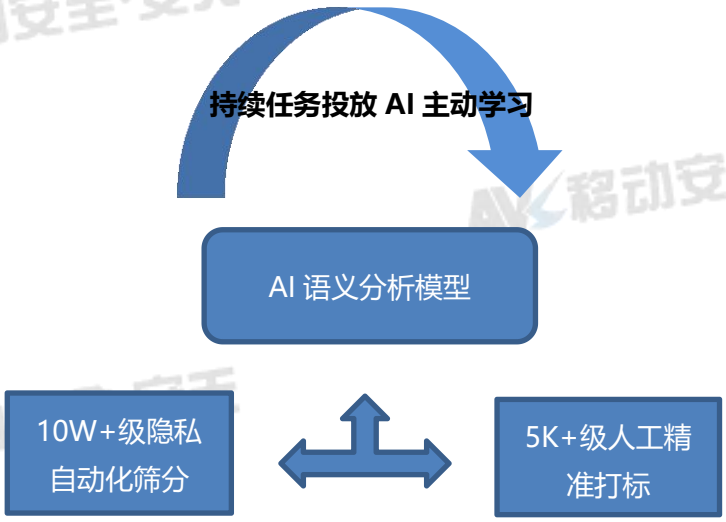

图 3.1 隐私政策语义分析模型能力迭代

当前对隐私政策能实现如下内容的检测：隐私政策的更新时间，个人信息的存储地点、时限，运营主体的名称、地址、联系方式，个人信息数据主体的权利、投诉渠道，个人信息收集/使用的目的、范围、方式，以及是否向第三方提供个人信息。

3.1.3 一流的安全运维能力体系

当下我们正处在持续进步、持续变化的安全环境下，评价和衡量一个产品不仅仅从产品的表象能力来评估，同时也需要评估产品的持续运维能力和企业投入规划。

安天经过十余年的发展，已经建立了一套顶尖的应用安全检测运维能力体系，具有约 30 人的专业安全分析团队，约 15 人的安全运维团队，以及配套的各类系统服务软硬件资源。在海量样本捕获、筛分、存储、分析判定和能力输出建立了完备的工程化体系，内部样本存储量过亿，恶意样本存量过千万，并持续投入继续运营和建设。

同时，为支撑移动应用用户权益保障检测系统的能力输出和持续迭代，组建了包含安全专家、系统架构师和高级研发工程师在内的团队进行系统知识库建设和持续的能力规划迭代输出。

3.1.4 丰富的产业链合作经验

用户权益保障的实现离不开上下游产业链的共同努力，净化移动互联网安全生态需要从源头出发，在监管和应用市场“双管齐下”。

安天多年来与工信、网信、公安等监管单位维持着长期、稳定的合作，涉及包括反病毒检测能力提供、移动互联网安全分析技术支撑、数据共享等领域。在本次用户权益保障合规系统建设中，我们也积极与监管侧沟通需求，推动方案的应用落地，希望为应用违规违法收集使用个人信息行为的治理提供能力，尽到安全厂商的社会责任。

在应用市场方面，安天在 2016 年就与国内知名手机厂商建立了合作关系，并将反病毒检测能力应用到了手机商场应用市场的上架审核环节，多年来持续为应用市场上架和用户终端提供安全防护能力。

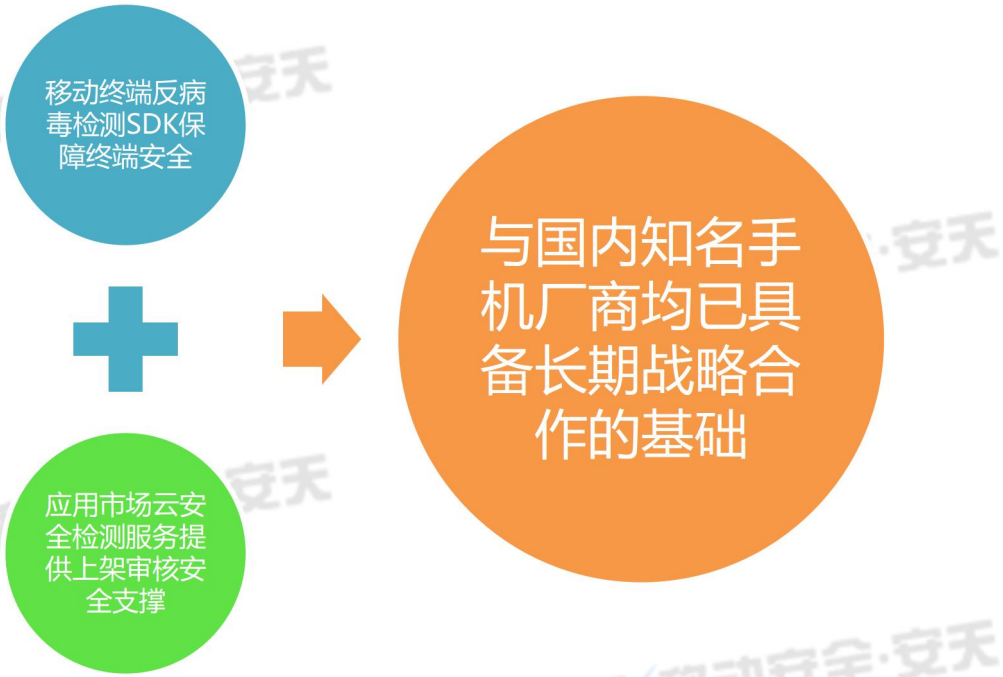

图 3.3 手机厂商合作基础框架

基于日趋重要的用户权益保障合规需求，安天有信心也有能力与手机厂商达成深化合作，把好移动终端用户权益保障合规的关口，从应用生态的源头着手，影响和规范开发者行为，维护广大移动终端用户权益。

3.2 产品价值

3.2.1 共同构建安全纯净移动应用生态

安天希望通过监管审核的上下游联通，共同构建安全纯净的移动应用生态。结合监管细化的认定标准以及现阶段的治理目标，通过安天的运维能力体系快速、准确的形成检测能力，形成用户权益保障合规基准能力，并通过手机厂商及潜在的三方应用市场的合作机会，落实上架审核规范和要求，最终完成上下游一体的综合整治目标。

图 3.4：用户权益保障合规整治驱动关系

通过实现上下游一体的综合治理，最终可以达到互惠双赢的目的，包括：

- 通过有效监管达到净化移动互联网应用生态，使广大终端用户受益
- 帮助应用上架合规审核能力的建设，避免监管通报，减少用户投诉，提高用户认可
- 树立了监管求真务实的形象，保障了应用市场安全、合规的口碑

3.2.2 降低合作伙伴的成本投入

用户权益保障合规检测系统为安天自建检测服务系统，使用 SaaS 方案通过公有云投放检测任务以及回调检测结果，可以有效降低成本投入，快速达到合规要求。

图 3.5 成本影响分析图

合作伙伴可根据需要，提前确认所需的检测项能力，并由安天配置定制化投放接口，并同步提供渠道 ID 和密钥。在合作伙伴提供 callback 地址，并完成配置联调后即可投放任务。

合作伙伴使用 HTTP 的 POST 方式，将需要检测的应用下载地址和应用对应隐私政策链接地址通过投放接口提交给系统，检测结果将通过回调地址传回。

为了保证系统服务的稳定性，需要对任务投放的数量和频率进行约定，具体可由商务合作洽谈根据实际情况协商，安天在确认投放量需求后会根据实际情况分配真机资源来保证任务的及时性。

第 4 章　关于安天移动安全

安天移动安全是安天科技集团旗下专注移动用户安全的科技公司。安天科技集团于 2000 年成立，是引领威胁检测与防御能力发展的网络安全国家队，是习总书记视察的唯一一家网络安全企业。

经过 10 年的技术积累，自主创新的安全引擎覆盖了超过 20 亿智能终端，成为国民级安全内核，为智能终端的用户生态实现全场景覆盖的移动应用安全治理，对导致用户权益受损的不良行为和黑灰产进行技术响应，并为开发者提供专业安全辅导和配套产品服务。

安天移动安全自主研发的移动反病毒引擎以 2013 全年最高平均检出率荣获 AV-TEST “移动设备最佳防护”奖，成为首获此项国际大奖的亚洲安全厂商，实现了中国安全厂商在全球顶级安全测评领域重量级奖项零的突破。2015 年，在 AV-C 的年度测评中，凭借全年两次 100%检测率的惊人成绩，再次冲顶。2018 和 2019 年，在 AV-TEST 的年度测评中，凭借全年 6 期病毒检测率皆为双 100%的领先成绩，三度领跑世界级移动安全杀毒领域。

近年来公司已申请国家专利 140 余项、PCT 专利 4 项，其中 1 项发明专利荣获湖北省专利金奖。公司主导的国家标准“移动互联网应用程序安全开发和生命周期管理指南”成功立项，并参与了多项行业标准的起草制定工作。经过多年发展，公司荣获湖北省政府颁发的湖北省科学技术奖、湖北省支柱产业细分领域隐形冠军企业、武汉市服务业领军企业、武汉市千企万人支持计划企业、武汉市软件百强企业等多项荣誉称号。

经过多年的不断努力，公司围绕核心技术优势与中央网信办，工信部，通信管理局，国家互联网应急中心，泰尔实验室等多个机构单位进行合作，为国家监管部门提供技术支撑，为华为、小米、OPPO、vivo 等智能设备厂商，以及猎豹移动，奇安信等企业客户提供安全引擎和技术赋能，目前已与全球知名芯片、移动智能终端、移动应用等产业链上下游上百家厂商成功合作。

截至目前，公司的反病毒引擎产品已为全球超过 30 亿移动智能终端设备的使用安全保驾护航，日活和月活用户分别突破 6 亿和 14 亿，已发展成为全球顶尖移动智能终端设备安全防护厂商。

未来，安天移动安全将通过自主创新国际顶级的安全核心技术，与产业终端厂商共同打造操作系统内生安全和基于开发者信誉平台的绿色生态链，为新时代用户打造国民级安全产品，在万物互联时代营造更安全和可持续的全场景健康数字体验。