厦门嘉佑安科信息技术有限公司

观澜 App 隐私合规检测

产品白皮书

(V1.0.0)

目 录

修订记录

版本	作者	日期	修订内容
V1.0.0	XXX	2024/5/23	创建文档

一、概述

1.1. 背景概述

近年来，随着互联网技术在全球的飞速发展，人类社会已被裹挟进“大数据”时代，个人信息安全问题也正日益困扰着所有人。个人信息的网络化和透明化已经成为不可阻挡的大趋势，但与此同时个人信息泄露情况不容乐观，手机移动应用过度采集个人信息呈现普遍趋势，消费者对这些存在诸多担忧，但往往缺乏足够有效的应对手段。同时个人信息泄露事件频出，保护消费者个人信息和个人信息安全工作亟待加强。在这样的背景下，移动应用隐私合规检测应运而生。

早在 2017 年，《网络安全法》就明确要求网络运营者应当加强个人信息保护、规范个人信息的收集、使用、存储、处理、传输等行为。2021 年实施的《个人信息保护法》则是我国首部针对个人信息保护的专门性法律，明确规定了企业收集、使用、处理、存储、共享、转让个人信息等行为应当遵循的原则和规范，以及违法行为的处罚等。

迄今为止，网信办、工信部、公安部等监管部门已经依照法律法规和部门规章要求，对 App 隐私合规问题启动了多轮执法或专项行动。种种迹象表明，对企业而言践行 App 隐私保护承诺已经刻不容缓。

1.2. 产品定位

观澜 App 隐私合规检测产品是我司针对 App、小程序、快应用、SDK 等可能出现的隐私合规风险而推出的专业隐私合规检测产品，该产品通过自动化检测+专家级人工检测的方式，对多类检测对象提供多方位、全面的隐私合规检测，并出具专业的隐私合规检测报告，可为应用运营者及开发者、应用市场和监管部门，提供专业、规范、精确、高效的隐私合规检测服务。

综上，本产品可以带来的安全价值有：

- 帮助应用开发者和运营者及时发现并纠正应用存在的违反法律法规的行为，避免承担法律责任和社会责任
- 帮助应用开发者和运营者尊重和保护用户的个人信息自主权，提高用户对应用的信任度和满意度
- 帮助应用开发者和运营者展示应用的安全合规水平，提升应用的品牌形象和市场竞争力动 App 安全加固及防御提供安全依据
- 帮助应用开发者和运营者防范和减少应用因个人信息泄露、被盗用、被滥用等造成的安全风险和损失
- 帮助应用市场对平台内上架的应用落实管理责任
- 促进监管部门对移动应用进行合规生态治理，保障个人信息安全

二、产品核心功能

观澜 App 隐私合规产品是针对 App、小程序、快应用、SDK 中出现个人信息的非法收集、滥用、泄露等严重问题，结合相关法律法规和监管要求，为监管机构、测评机构、应用开发企业等推出的合规检测服务。该平台针对移动应用的基本信息、漏洞信息、收集和使用个人信息行为、通讯传输行为、软件和技术供应链情况、技术脆弱性、隐私政策规范性等进行多维度安全检测和合规检测，并出具专业的个人信息安全报告。帮助监管机构准确、有效地提供行政执法依据，帮助测评机构出具专业的个人信息测评报告，帮助应用开发企业在应用发布前评估个人信息的安全性和合规性。

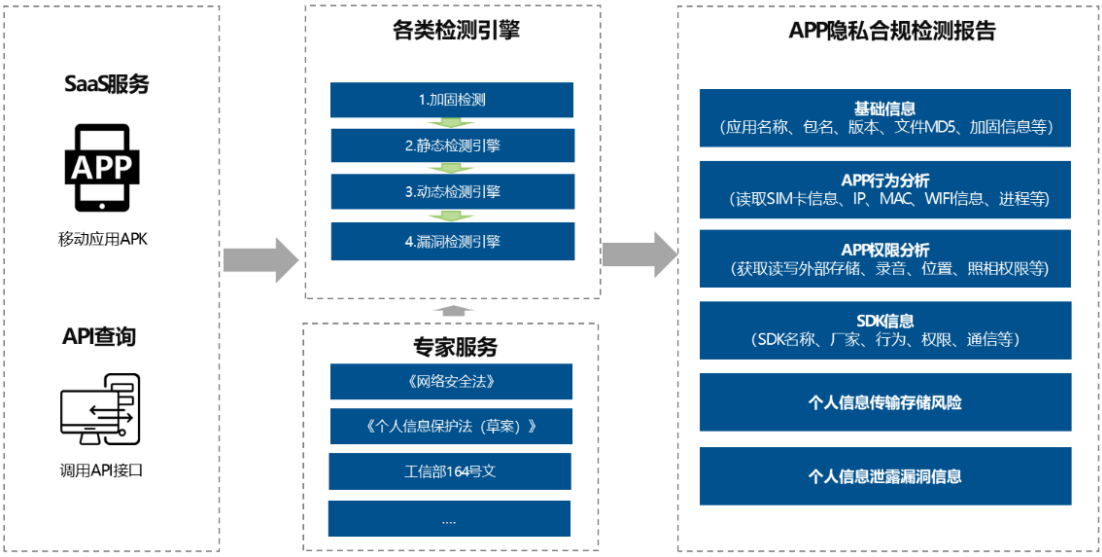
主要检测内容如下：

1）行为合规检测：基于 AI、静动态检测，针对 APP 的隐私数据采集等行为进行识别，依据国家相关法规及规范检测行为合规性。

2）权限合规检测：基于静动态检测，对各类权限进行识别，检测敏感权限使用合规性。

3）第三方 SDK 合规检测：大数据结合静动态检测，对于 APP 集成的第三方 SDK 的隐私合规性进行检测，并提供代码漏洞分析。

2.1. 检测流程



观澜 App 隐私合规检测产品的服务模式是通过 SaaS 控制台提供服务，用户只需要登录平台，上传 App 即可进行隐私合规检测。

平台会把 App 上传到检测系统进行加固判断，如果已加固则进行脱壳处理，再通过静态检测引擎、动态检测引擎、漏洞检测引擎等进行自动化检测，与此同时安全专家团队会依据自己对法律法规的理解，对自动化报告进行人工复查，以免出现误报、漏报，且使报告更精准、更全面。

2.2. 应用基本信息检测

1）检测内容：

检测项	检测目的	检测说明
应用名称	获取应用名称	获取应用名称并展示
包名	获取应用包名	获取应用包名
文件大小	获取应用文件大小	获取应用文件大

		小
版本信息	获取应用版本	获取应用版本
targetSdkVersion	获取 SDK 编译版本	获取 SDK 编译版本
文件 MD5	获取应用文件 MD5	获取应用文件 MD5
文件签名	获取应用文件签名信息	获取应用文件签名信息
加固厂商	获取应用加固厂商	获取应用加固厂商

2）技术原理：

- 使用工具 aapt 获取 APK 的应用程序名称、包名、版本号、主 Activity
- 使用文件读取类获取文件大小
- 使用 MD5 工具类获取 APK 的 MD5 信息
- 使用 keytool 获取 APK 的签名信息

2.3. 自动化+专家级测评项目

观澜 App 隐私合规检测平台为企业用户、测评机构、监管部门、应用市场提供多维度的超过百项检测点，本产品白皮书中仅列举部分检测项目如下：

序号	检测类型
1	违规收集个人信息
2	超范围收集个人信息

3	违规使用个人信息
4	违规索取权限
5	未按法律规定提供删除或更正个人信息功能
6	隐私数据出境
7	App、SDK 自启动和关联启动

2.4. 动态生成检测报告

平台依据检测项目进行检测并自动动态生成检测报告 ,检测完成后可以在线查看检测结果及对应的检测报告 , 并且提供用户自定义报告展示内容框架、封面样式、页眉内容、报告水印的功能。

当用户下载报告时 , 无需人工干预即可直接动态生成 , 解决了传统测评业务中需要大量人工撰写检测报告的问题。

同时 , 报告中针对检测出现的隐私合规问题 , 提供由安全技术专家给出的专业整改建议，为应用开发者降低合规成本，提高应用上架的成功率。

2.5. 风险 App 排名

平台提供风险 App 排名功能，可以对在平台进行隐私合规检测的 App 中出现的隐私合规问题进行分析统计，协助客户了解 App 隐私合规问题的分布情况及趋势。

2.6. 风险类型排行

平台提供风险类型排行功能 ,可以对系统中应用的隐私合规问题类型进行分析统计，协助客户了解隐私合规问题的风险类型分布情况。

2.7. App 检测地域分布

平台可以分析统计进行隐私合规检测的开发者或者企业的所在地域 ,协助客户全面了解 App 隐私合规问题现状。

2.8. App 类型风险分布

平台可以统计、分析进行隐私合规检测的 App 类型分布情况，协助客户多方位了解各行业应用发展现状。

2.9. 系统管理与升级

系统提供专业的系统授权管理和服务升级机制 ,通过用户及角色管理机制对系统使用者进行权限控制 , 提高系统使用安全性 ; 另外随着最新的安全技术迭代和检测技术更新，系统支持升级更新以保证最新的安全技术服务于用户。

三、应用场景

3.1. 应用运营者及开发者

3.1.1. 业务描述

应用开发者、运营者，在应用上架、版本更新时，需要全面检查应用隐私合规问题，以达到降低合规成本，减少通报下架风险的目的。

3.1.2. 行业痛点

- 无法承担独立部署的开销
- 无法承担维护安全团队的开销
- 无法对当前应用的隐私合规问题实现全面检查并准确定位、修复问题

3.2. 应用市场

3.2.1. 业务描述

应用市场为确保平台内上架的应用符合监管机构的要求以及国家法律法规的规定，需要对海量应用进行隐私合规检测。

3.2.2. 行业痛点

- 人工测试成本高、效率低，不能满足企业的需要
- 快速的自动化检测平台可保障持续进行版本测试、迭代
- 可独立部署，保证数据、应用代码的安全性

- 无法对当前应用的隐私合规问题实现全面检查并准确定位、修复问题

3.3. 测评机构

3.3.1. 业务描述

国家相关测评机构需要检测企业发布的 App 是否符合国家的相关法律法规要求，从而需要对送检的大量应用进行隐私合规检测。

3.3.2. 行业痛点

- 快速的自动化检测平台可有效的处理对大量应用进行隐私合规检测的需求
- 可独立部署，保证数据、应用代码的安全性
- 无法对当前应用的隐私合规问题实现全面检查并准确定位、修复问题

3.4. 监管部门

3.4.1. 业务描述

国家监管部门需要对当前市场的应用进行全面的合规检查 ,以达到对 App 形成常态化监管，促进 App 合规生态治理，提升个人信息保护力度的目的。

3.4.2. 行业痛点

- 行业丰富，且 App 数量巨大，人工检测无法满足需求，需要快速的自动化检测
- 快速的自动化检测平台可有效的检测大量 App 并进行统计、分析

- 可独立部署，保证数据、应用代码的安全性
- 无法对当前应用的隐私合规问题实现全面检查并准确定位、修复问题

四、产品优势

1）检测范围广泛：提供多维度的超过百个检测点，检测范围覆盖违规手机个人信息、违规索取权限、违规使用个人信息、超范围收集个人信息等。有效地发现应用中的隐私合规问题，并准确定位问题出现的源头，助力开发者识别和解决 App 中存在风险，有效保护移动应用的合规性。

2）检测能力专业：静态、动态检查技术与专家级人工检查相结合，检测结果准确率提升，专家级整改指导更专业聚焦。

3）检测精准高效：自动化隐私风险的检测，替代人工代码翻查，高效交付检测报告，精准定位 App 存在的隐私风险点。

4）检测规范全面：检测依据全面覆盖国家网信办、工信部、公安部、市场监管总局四部委发布的 14 个相关法律法规。

5）检测技术先进：依托成熟的技术体系，采用业内主流的人工智能 NLP 自然语言处理和自研沙箱检测等多项先进技术。

6）检测的可扩展性：除了内置的近百个检测点外，平台还将依据国家相关法律法规后续的变更或补充，提供检测项的扩展和更新服务，从而保证平台可以及时满足最新的合规测试要求。

7）用户数据隐私的保护：可支持本地独立部署，全面隔离用户应用信息及测评结果，保护用户数据的隐私性及安全性。

8）感知合规风险的趋势：采用机器学习和大数据分析技术，AI 赋能可视化呈现移动隐私安全态势，主动发现隐私风险，并且可对检测的应用结果进行批量统计，获取应用中的合规风险分布及趋势。

五、公司简介

厦门嘉佑安科信息技术有限公司（下称：嘉佑安科）位于海上花园城市—厦门，注册资金人民币 1000 万元。在厦门、深圳、武汉三地设有研发中心，是一家致力于打造完善的隐私安全合规产品研发和技术运营管理体系，保护人民隐私安全合规的安全服务商。嘉佑安科母公司是国家高新技术企业、福建省重点上市后备企业、福建省数字经济核心产业领域未来独角兽企业、福建省科技小巨人领军企业、福建省互联网最具成长型企业、厦门十大科创板潜力企业、厦门市重点软件和信息服务企业，现拥有 150 项软著和专利。

公司坚守以“成为人民隐私安全的忠诚守护者”为企业愿景，勇担“保护国家安全、社会和谐稳定、保护人民合法权益”的企业使命，发展规划始终以人民根本利益为中心，通过发挥技术优势、专业的安全服务，为用户、政府、企业、开发者和消费者打造安全、稳固、可信的网络空间生态环境。