

# 灵鲲 APP 隐私合规 产品白皮书



# 目录

1. 背景.....	3
1.1 背景概述.....	3
1.2 监管介绍.....	4
2. 产品介绍.....	5
2.1 产品概述.....	5
2.2 检测流程.....	6
2.3 检测内容.....	6
2.3.1 应用基本信息检测.....	6
2.3.2 APP 违法行为检测.....	8
2.3.3 APP 违法权限检测.....	9
2.3.4 第三方 SDK 检测.....	12
2.3.5 APP 通信传输.....	13
2.3.6 APP 数据存储.....	16
2.3.7 APP 源文件安全.....	18
2.3.8 身份认证风险.....	20
2.4 技术优势.....	21
2.4.1 动态检测技术.....	21
2.4.2 云手机技术.....	21
3. 产品价值.....	22

# 1. 背景

## 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亟待加强。

同时，随着国家对个人信息安全的愈发重视，国家、行业等不同层级的监管机构都出台了一系列的法律法规和行业规范，用于净化移动应用个人信息安全市场。

相关法律法规的出台，为移动应用展开业务的同时，如何收集、使用、存储、传输、销毁个人信息数据进行了规定。同时定义了个人信息安全条款的必要标准和格式以及在第三方使用数据时必要的流程。相关法律法规也为监管机构和检测机构等给出了合规检测标准，为相关检测工具定义了检测依据。

## 1.2 监管介绍



目前,主要的监管单位是工信部、网信办以及公安部。据相关统计,2020年市面上APP的总数为325万款,工信部2020年已经完成了44万款APP的隐私合规检测。并计划2021年完成180万款APP的隐私合规检测,除去下载量较低的APP,180万款APP基本覆盖了目前市面上所有主流的移动应用。截止2021年7月,工信部已经通报了第五批违规APP名单,预计全年通报十四批。

网信办虽然介入较晚,但监管力度非常大,例如7月5日通报的某滴事件,不仅勒令APP下架,还禁止新用户注册。另外还有各省网信办相继通报管辖范围内的APP违规事件,并勒令相关企业整改与说明。

公安部的通报与工信部、网信办不同的是,更多采用线下的方式执法。例如近期深圳公安对线上教育APP进行了集中整治,其方式是对APP的运营企业进行线下口头警告,勒令整改,否者传唤并强制下架。

不论是工信部、网信办还是公安部,其监管力度都非常大,可以看出国家层面对APP违法违规收集用户隐私的行为是零容忍态度。对于企业而言,提前自查、整改并满足合规要求,成为了亟待解决的问题。

## 2. 产品介绍

### 2.1 产品概述



#### 行为合规检测

对APP违法收集用户隐私的行为进行合规检测

#### 权限合规检测

对APP的敏感权限使用情况进行检测，判断其是否合规

#### 第三方SDK合规检测

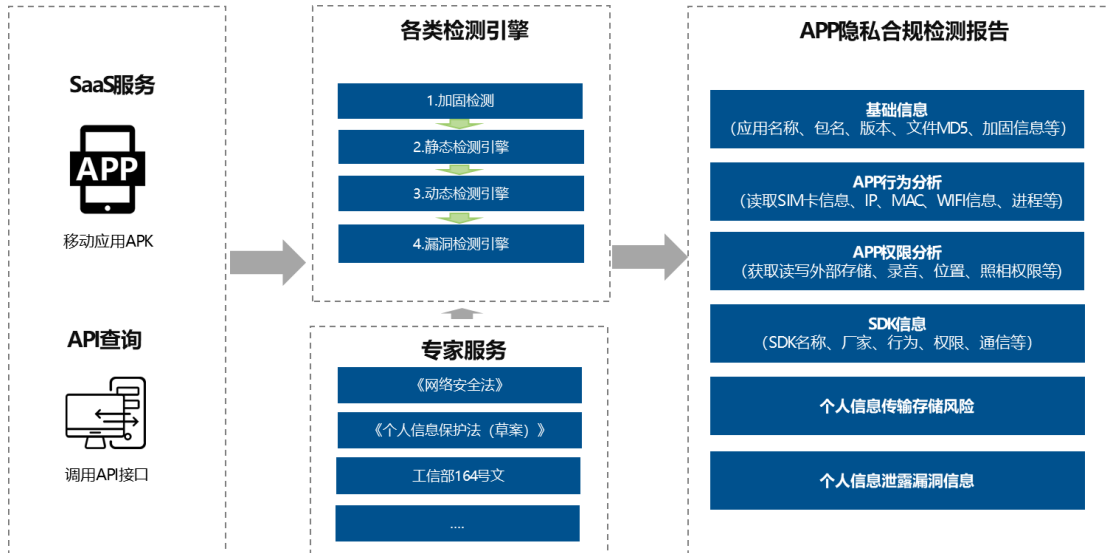
对第三方SDK的行为、权限、通信等内容进行合规检测

灵鲲 APP 隐私合规产品是针对移动应用、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。

## 2.2 检测流程



灵鲲 APP 隐私合规产品有两种服务模式：第一种是通过腾讯云 SaaS 控制台提供服务，客户只需要登录控制台，上传 APP 即可进行隐私合规检测。第二种是客户通过 API 方式连接到灵鲲 APP 隐私合规系统，通过 API 上传 APP，并获取报告。第一种适用拥有 APP 数量不多的客户，第二种适用拥有 APP 数量较多的客户或监管单位。

不论是哪种服务模式，最终都会把 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，与此同时腾讯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。

## 2.3 检测内容

### 2.3.1 应用基本信息检测

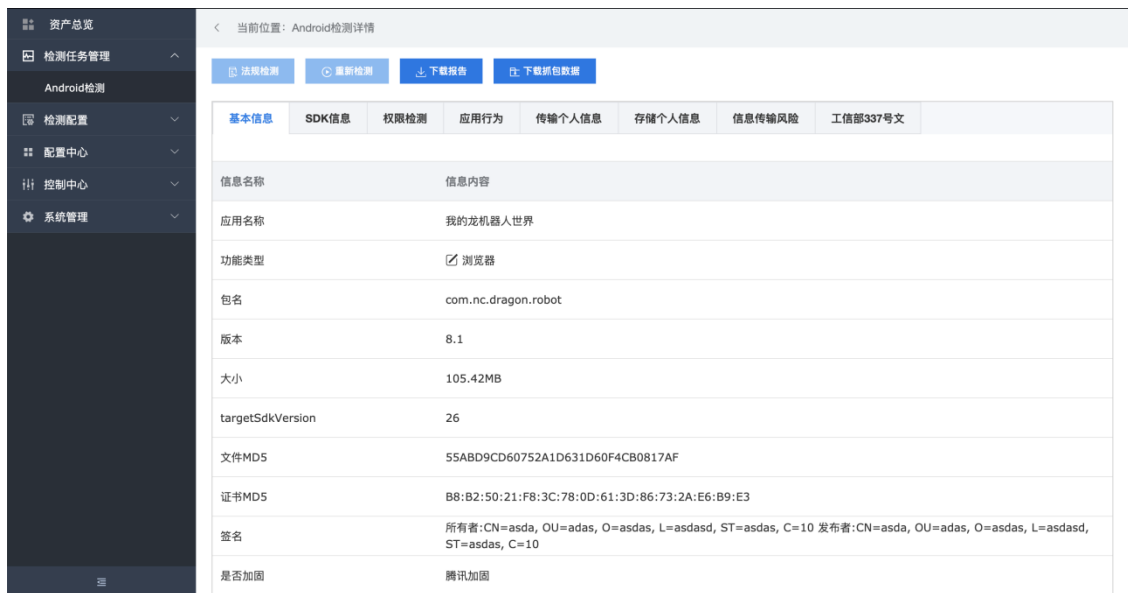
- 技术说明

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
签名信息	获取应用签名信息	获取应用签名信息
加固厂商	获取应用加固厂商	获取应用加固厂商

■ 技术原理

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

■ 效果展示



## 2.3.2 APP 违法行为检测

序号	检测项	备注
1	违规收集个人信息	该检测项包含 8 个细分场景检测
2	超范围收集个人信息	该检测项包含 8 个细分场景检测
3	违规使用个人信息	该检测项包含 2 个细分场景检测
4	强制用户使用定向推送功能	该检测项包含 2 个细分场景检测
5	APP 强制、频繁、过度索取权限	该检测项包含 7 个细分场景检测
6	APP 频繁自启动和关联启动	该检测项包含 3 个细分场景检测



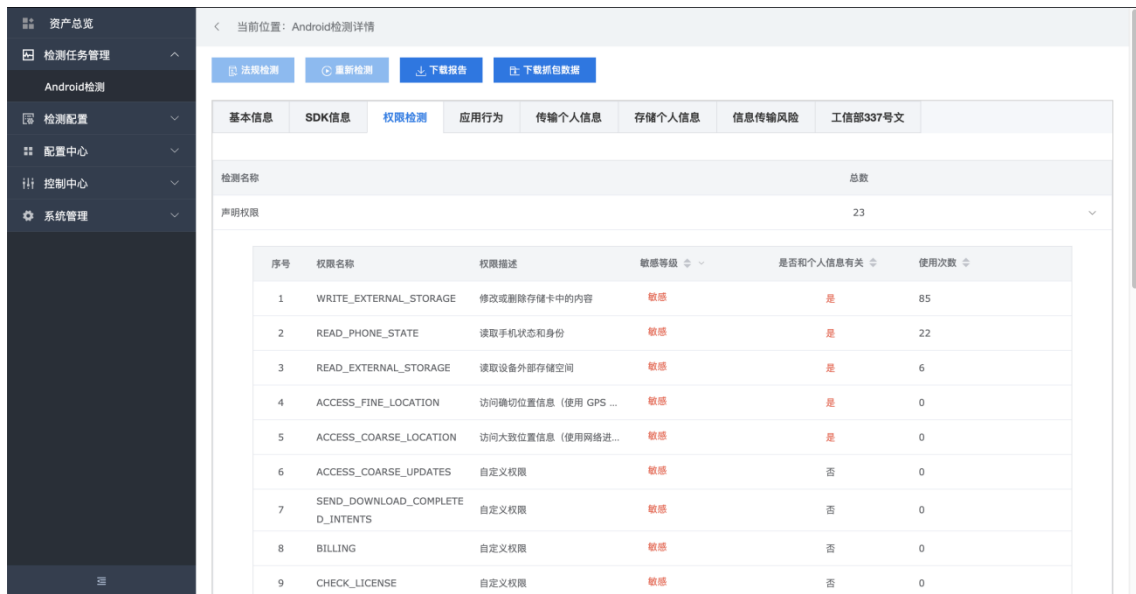
## 2.3.3 APP 违法权限检测

### 2.3.3.1 声明权限

#### ■ 技术原理

通过反编译 APK 包, 获取 AndroidManifest.xml 文件, 检测应用在 AndroidManifest.xml 文件中配置的权限, 即声明的权限, 包括谷歌官方权限、应用开发者定义的权限。

#### ■ 效果展示



The screenshot shows a web-based interface for Android permission detection. The left sidebar contains navigation options: 资产总览, 检测任务管理, Android检测, 检测配置, 配置中心, 控制中心, and 系统管理. The main content area is titled '当前位置: Android检测详情' and includes buttons for 法规检测, 重新检测, 下载报告, and 下载脱包数据. Below these are tabs for 基本信息, SDK信息, 权限检测 (selected), 应用行为, 传输个人信息, 存储个人信息, 信息传输风险, and 工信部337号文. A table shows the results for '声明权限' (Declared Permissions) with a total of 23 items. The table columns are: 序号 (Serial Number), 权限名称 (Permission Name), 权限描述 (Permission Description), 敏感等级 (Sensitivity Level), 是否和个人信息有关 (Related to Personal Information), and 使用次数 (Usage Count).

序号	权限名称	权限描述	敏感等级	是否和个人信息有关	使用次数
1	WRITE_EXTERNAL_STORAGE	修改或删除存储卡中的内容	敏感	是	85
2	READ_PHONE_STATE	读取手机状态和身份	敏感	是	22
3	READ_EXTERNAL_STORAGE	读取设备外部存储空间	敏感	是	6
4	ACCESS_FINE_LOCATION	访问确切位置信息 (使用 GPS ...	敏感	是	0
5	ACCESS_COARSE_LOCATION	访问大致位置信息 (使用网络进...	敏感	是	0
6	ACCESS_COARSE_UPDATES	自定义权限	敏感	否	0
7	SEND_DOWNLOAD_COMPLETE_D_INTENTS	自定义权限	敏感	否	0
8	BILLING	自定义权限	敏感	否	0
9	CHECK_LICENSE	自定义权限	敏感	否	0

### 2.3.3.2 敏感权限风险

#### ■ 技术原理

通过反编译 APK 包, 获取 AndroidManifest.xml 文件, 检测应用在 AndroidManifest.xml 文件中配置的权限, 权限的等级为敏感等级。

#### ■ 效果展示

序号	权限名称	权限描述	敏感等级	是否和个人信息有关	使用次数
1	WRITE_EXTERNAL_STORAGE	修改或删除存储卡中的内容	敏感	是	85
2	READ_PHONE_STATE	读取手机状态和身份	敏感	是	22
3	READ_EXTERNAL_STORAGE	读取设备外部存储空间	敏感	是	6
4	ACCESS_FINE_LOCATION	访问确切位置信息 (使用 GPS ...)	敏感	是	0
5	ACCESS_COARSE_LOCATION	访问大致位置信息 (使用网络进...)	敏感	是	0
6	ACCESS_COARSE_UPDATES	自定义权限	敏感	否	0
7	SEND_DOWNLOAD_COMPLETE_D_INTENTS	自定义权限	敏感	否	0
8	BILLING	自定义权限	敏感	否	0

### 2.3.3.3 尝试使用未声明权限

#### ■ 技术原理

通过反编译 APK 包, 获取 AndroidManifest.xml 文件, 检测应用在 AndroidManifest.xml 文件中配置的权限, 获取声明权限。再通过动态沙箱检测, 获取应用权限行为数据, 进行对比, 获取尝试使用未声明权限。

#### ■ 效果展示

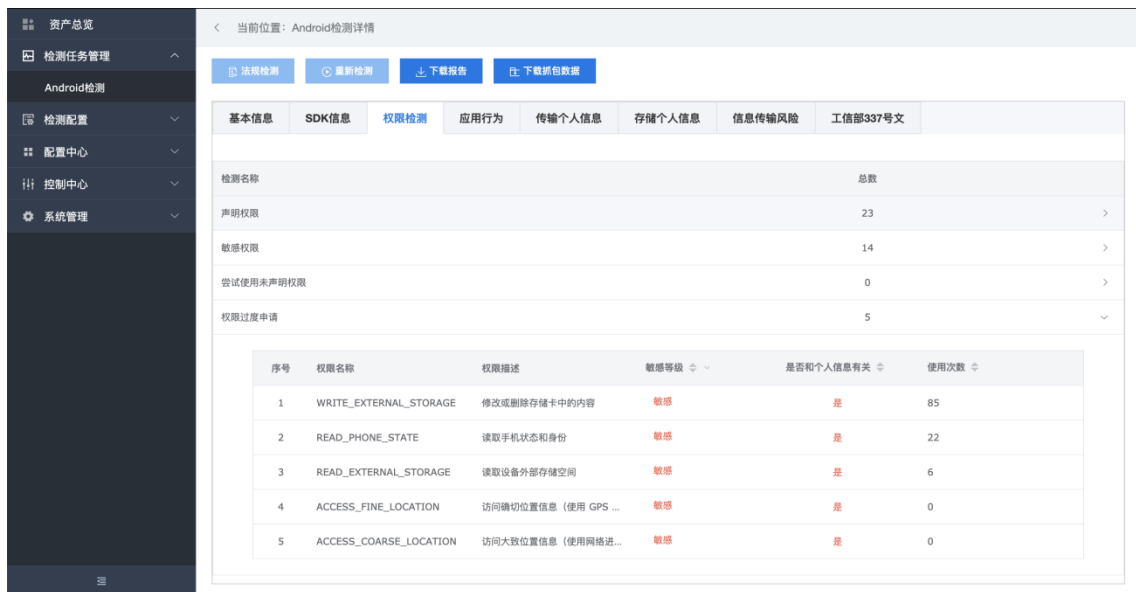
序号	权限名称	权限描述	敏感等级	是否和个人信息有关	使用次数
1	WRITE_SETTINGS	修改系统设置	敏感	否	173

### 2.3.3.4 过度声明风险

#### ■ 技术原理

通过反编译 APK 包, 获取 AndroidManifest.xml 文件, 检测应用在 AndroidManifest.xml 文件中配置的权限, 与行业最小权限库相对比, 判断是否存在权限过度申请行为。

#### ■ 效果展示



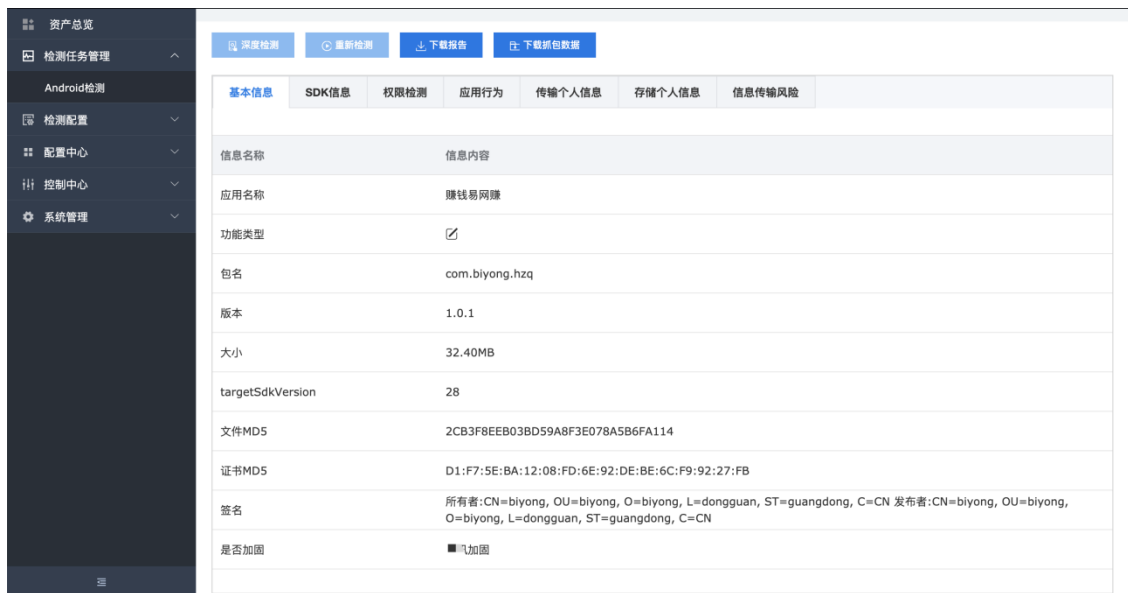
序号	权限名称	权限描述	敏感等级	是否和个人信息有关	使用次数
1	WRITE_EXTERNAL_STORAGE	修改或删除存储卡中的内容	敏感	是	85
2	READ_PHONE_STATE	读取手机状态和身份	敏感	是	22
3	READ_EXTERNAL_STORAGE	读取设备外部存储空间	敏感	是	6
4	ACCESS_FINE_LOCATION	访问确切位置信息 (使用 GPS ...	敏感	是	0
5	ACCESS_COARSE_LOCATION	访问大致位置信息 (使用网络进...	敏感	是	0

### 2.3.3.5 APP 安全加固情况

#### ■ 技术原理

检测 APK 包中加固后的 so 库的名称, 通过识别不同厂商的固定特征, 判断 APK 的加固厂商。

#### ■ 效果展示



## 2.3.4 第三方 SDK 检测

### 2.3.4.1 SDK 分析

#### ■ 技术原理

通过反编译 APK 包，对比 SDK 库，检测应用在代码中引用的 SDK 包名；在应用动态运行时，触发的行为的函数调用栈与 SDK 库进行对比，检测应用在运行时使用的 SDK 数据。

#### ■ 效果展示

序号	SDK名称	包名	SDK厂商	SDK描述	SDK类型
1	百川云旺-即时通讯	com.alibaba.sdk.android	阿里巴巴集团控股有限公司	高稳定性即时通讯方案	其他
2	阿里云HTTPDNS	com.alibaba.sdk.android.h...	阿里云计算有限公司	HTTPDNS是面向移动开发者推出的一款域名解析产品, 具有...	其他
3	QQ互联	com.tencent.StubShell	深圳市腾讯计算机系统有限公司	--	社交
4	腾讯开发插件库	com.tencent.connect	腾讯	腾讯推出的授权库, 用于用户登录操作。	社交
5	友盟移动统计	com.umeng.analytics	北京锐讯灵通科技有限公司	统计分析组件可精准统计应用的新增、启动、活跃、自定义事...	统计
6	腾讯Bugly升级SDK	com.tencent.bugly.beta	深圳市腾讯计算机系统有限公司	升级功能是为App的灰度升级而开发的组件, 在bugly内测...	其他
7	友盟消息推送	com.umeng.message	北京锐讯灵通科技有限公司	消息推送组件, 提供给用户准时的Push通知功能, 聚合小米、...	推送
8	支付宝支付	com.alipay	蚂蚁金融服务集团	--	支付
9	QQ互联	com.tencent.taauth	深圳市腾讯计算机系统有限公司	接入QQ互联平台, 让你的移动应用支持QQ账号登录、分享到...	社交
10	支付宝支付	com.alipay.sdk	支付宝网络有限公司	iOS、Android应用嵌入APP支付SDK, 用户支付时唤起支付...	支付
11	腾讯Bugly崩溃分析	com.tencent.bugly	腾讯公司	腾讯Bugly, 为移动开发者提供专业的异常上报和运营统计, ...	统计

## 2.3.5 APP 通信传输

### 2.3.5.1 启用 VPN 服务检测

#### ■ 技术原理

检测目的	检测应用是否可以启动 VPN 服务。
风险等级	低
威胁描述	使用 VPN 联网时, 通过网络请求的数据容易被劫持, 造成用户敏感信息泄露。可以提供 VPN 服务的软件, 又叫“翻墙”软件。提供“翻墙”服务属于违法行为。
解决方案	建议开发者自查, 应用中不要启动 VPN 服务。

#### ■ 效果展示

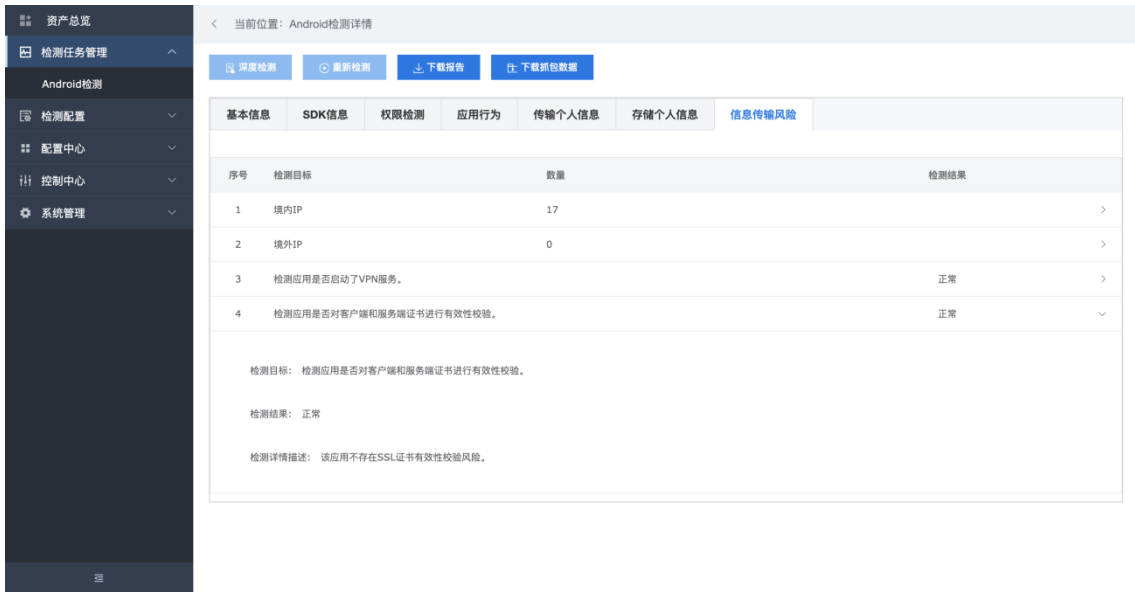


### 2.3.5.2 SSL 证书有效性风险

#### ■ 技术原理

检测目的	检测应用是否对客户端和服务端证书进行有效性校验。
风险等级	中
威胁描述	<p>使用 HTTPS 协议时，客户端必须对服务器证书进行完整性校验，以验证服务器的合法性。如果未校验，客户端可能与仿冒的服务器建立通信链接，同时服务端也可能与仿冒的客户端建立通信链接，即“中间人攻击”。Android 允许开发者重定义证书验证方法，使用 X509TrustManager 类检查证书是否合法并且是否过期。如果重写 X509TrustManager 时，checkServerTrusted()方法对证书校验结果未做任何处理，即在证书验证失败时，仍然与服务器建立通信链接，存在发生“中间人攻击”的风险。当发生中间人攻击时，仿冒的中间人可以冒充服务器与客户端进行交互，同时冒充客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号码、账号、密码等敏感信息，甚至可能对通信内容进行篡改。</p>

#### ■ 效果展示



### 2.3.5.3 访问境外服务器风险检测

#### ■ 技术原理

检测目的	检测应用中 ip、域名是否访问境外服务器。
风险等级	高
威胁描述	应用程序访问境外服务器造成网络请求延迟、卡顿，被防火墙屏蔽网络请求出现访问无响应。

#### ■ 效果展示



### 2.3.5.4 HTTP 传输通道风险检测

## ■ 技术原理

检测目的	检测应用是否使用 HTTPS 协议对传输通道进行加密。
风险等级	低
威胁描述	由于 HTTP 数据传输是明文传输的，导致 HTTP 数据容易被抓取、篡改，泄露用户的敏感数据，如账号、密码等。甚至通过中间人劫持将原有信息替换成恶意链接或恶意代码程序，以达到远程控制、恶意扣费等攻击意图。

## ■ 效果展示

基本信息 权限检测 SDK信息 应用行为 **个人信息风险漏洞** 合规风险 APP违法违规收集使用个人信息自评估指南

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
> 4	WebView明文存储密码风险检测	数据存储风险	高	安全
√ 5	HTTP传输通道风险检测	通信传输风险	低	安全

检测目标: 检测应用是否使用HTTPS协议对传输通道进行加密。

检测结果: 安全

检测详细描述: 该应用没有使用HTTP协议进行数据传输。

## 2.3.6 APP 数据存储

### 2.3.6.1 WebView 明文存储密码风险检测

## ■ 技术原理

检测目的	检测应用的 WebView 组件中是否使用明文保存用户名及密码。
风险等级	高
威胁描述	WebView 组件默认开启了密码保存功能，会提示用户是否保存密



	码, 当用户选择保存在 WebView 中输入的用户名和密码, 则会被明文保存到应用数据目录的 databases/webview.db 中。攻击者可能通过 root 的方式访问该应用的 WebView 数据库, 从而窃取本地明文存储的用户名和密码。
--	---

■ 效果展示

基本信息 权限检测 SDK信息 应用行为 **个人信息风险漏洞** 合规风险 APP违法违规收集使用个人信息自评估指南

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
√ 4	WebView明文存储密码风险检测	数据存储风险	高	安全

检测目标: 检测应用的WebView组件中是否使用明文保存用户名及密码。

检测结果: 安全

检测详细描述: 该应用不存在明文存储密码漏洞。

### 2.3.6.2 密钥硬编码风险检测

■ 技术原理

检测目的	检测应用是否存在密钥硬编码风险。
风险等级	高
威胁描述	<p>密钥硬编码是指在代码中直接将加密算法的密钥设置为一个固定值。加密算法本身都是公开的, 加密内容的安全主要依赖于加密密钥。当密钥被硬编码在代码中时, 攻击者可以通过反编译得到密钥, 从而破解加密数据, 获取加密前的明文信息。密钥硬编码, 可直接造成加密数据被破解, 客户端与服务器之间的通信内容被破解, 导致应用内的加密文件被破解, 或是用户的敏感信息泄露。</p>

■ 效果展示

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
> 4	WebView明文存储密码风险检测	数据存储风险	高	安全
> 5	HTTP传输通道风险检测	通信传输风险	低	安全
∨ 6	密钥硬编码风险检测	数据存储风险	高	安全

检测目标: 检测应用是否存在密钥硬编码风险。

检测结果: 安全

检测详细描述: 该应用不存在密钥硬编码漏洞。

## 2.3.7 APP 源文件安全

### 2.3.7.1 资源文件泄露风险检测

#### ■ 技术原理

检测目的	检测应用中的资源文件是否存在被查看分析风险。
风险等级	中
威胁描述	程序在未进行资源文件加密时，直接把 APK 解压缩或者反编译会造成 APK 的资源文件被窃取、查看分析的风险。

#### ■ 效果展示

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
> 4	WebView明文存储密码风险检测	数据存储风险	高	安全
> 5	HTTP传输通道风险检测	通信传输风险	低	安全
> 6	密钥硬编码风险检测	数据存储风险	高	安全
∨ 7	资源文件泄露风险检测	源文件安全	中	安全

检测目标: 检测应用中的资源文件是否存在被查看分析风险。

检测结果: 安全

检测详情描述: 该应用不存在资源文件泄露风险。

### 2.3.7.2 Java 代码反编译风险检测

#### ■ 技术原理

检测目的	检测应用是否存在被反编译后泄露源代码的风险。
风险等级	高
威胁描述	Android 应用如果未采用有效的保护措施，可能面临被反编译的风险。反编译是将二进制程序转换成人们易读的一种描述语言的形式，是逆向工程中的常见手段。反编译的结果是易读的应用程序代码，这样就暴露了 Android 应用客户端的所有逻辑，比如与服务端的通讯方式、加解密算法、密钥、转账业务流程、软键盘技术实现等等。攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；绕过业务安全认证流程，直接篡改用户账号信息等。

#### ■ 效果展示

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
> 4	WebView明文存储密码风险检测	数据存储风险	高	安全
> 5	HTTP传输通道风险检测	通信传输风险	低	安全
> 6	密钥硬编码风险检测	数据存储风险	高	安全
> 7	资源文件泄露风险检测	源文件安全	中	安全
> 8	输入监听风险检测	身份认证风险	中	安全
√ 9	Java代码反编译风险检测	源文件安全	高	存在风险

检测目标: 检测应用是否存在被反编译后泄露源代码的风险。

检测结果: 存在风险

检测详情描述: 该应用使用了加固保护, 但加固强度不够, 比较容易被反编译后获取源代码。

修复建议: 建议使用专业应用安全加固方案, 对APK包中的classes.dex文件进行保护, 防止应用被反编译。

## 2.3.8 身份认证风险

### 2.3.8.1 输入监听风险检测

#### ■ 技术原理

检测目的	检测应用在敏感数据输入时是否使用不安全的系统键盘。
风险等级	中
威胁描述	客户端的敏感界面如登录界面、注册界面、支付界面等, 用户在输入敏感信息与显示 (输出) 时, 如果未使用安全键盘, 而使用第三方未知键盘或系统键盘的话可能存在数据被拦截与监听的风险, 导致账号、密码等敏感数据泄露。

#### ■ 效果展示

序号	漏洞名称	漏洞类型	风险等级	检测结果
> 1	启用VPN服务检测	通信传输风险	低	安全
> 2	SSL证书有效性风险检测	通信传输风险	中	安全
> 3	访问境外服务器风险检测	通信传输风险	高	安全
> 4	WebView明文存储密码风险检测	数据存储风险	高	安全
> 5	HTTP传输通道风险检测	通信传输风险	低	安全
> 6	密钥硬编码风险检测	数据存储风险	高	安全
> 7	资源文件泄露风险检测	源文件安全	中	安全
√ 8	输入监听风险检测	身份认证风险	中	安全

检测目标: 检测应用在敏感数据输入时是否使用不安全的系统键盘。

检测结果: 安全

检测详细描述: 该应用不存在系统键盘使用风险。

## 2.4 技术优势

### 2.4.1 动态检测技术

腾讯自主研发的沙箱系统，可监测 APP 在运行过程中的高达 100+ 种行为，包括读取文件、写入文件、获取应用进程、读取系统配置等行为。通过行为函数调用栈对行为主体进行分析，过滤 APP 或 SDK 行为，针对性排查违规行为主体，定位行为触发的代码位置。

### 2.4.2 云手机技术

云手机卡板机箱和服务器一起部署在腾讯云，通过网络将手机设备放到云端，借助设备管理平台 (STF) 对线上设备进行授权、管理，并且提供丰富的可视化操作云手机的支持，解决了只能依赖本地真机设备检测的问题，丰富了设备的可选择渠道（本地真机、云手机）、增强了个人信息检测产品的可用性和可操作性，同时，减去了本地手机设备的采购和管理成本。

### 3. 产品价值

- 合规价值

灵鲲 APP 隐私合规检测服务,可以有效满足工信部、网信办、公安部以及其他行业监管的合规要求,降低被监管单位通报的风险。

- 业务价值

灵鲲 APP 隐私合规检测服务,确保整改后的 APP 能够上线应用宝、小米、华为、OPPO、VIVO 等应用商店,保障业务连续性。

- 品牌价值

灵鲲 APP 隐私合规检测服务,可以帮助企业避免因监管通报而造成的负面影响,保护企业经营信誉和用户口碑。