百度移动应用安全治理平台

（百度安全）

一、概述

（一）方案背景

随着移动互联网和物联网的快速发展，移动应用和 IoT 应用已非常普及，随之而来的是针对 APP 的安全事件。据统计每年有 150 万种恶意 APP 软件、1600 万起恶意攻击事件，70%的 APP 存在安全漏洞问题。针对 APP 攻击的表现形式如暗中扣费、偷跑流量、恶意广告、窃取数据等，这些事件严重影响了 APP 厂商的口碑、损伤用户利益，所以保护 APP 安全刻不容缓。

另一方面，国家近几年加强对 APP 的监管力度，涉及金融、教育、医疗等，未来还将会持续扩大监管行业范围。各监管部门先后发布一系列法规、政策文件，规范 APP 收集使用个人信息的乱象行为，具体包括《网络安全法》《GB/T 信息安全技术个人信息安全规范》《APP 违法违规收集使用个人信息行为认定方法》《纵深推进 APP 侵害用户权益专项整治行动》等，并成立 APP 安全治理小组开展监管通报工作。根据统计，截至目前，仅工信部就发出了 20 余批次的点名通报，涉及千余款违规 APP，违规的 APP 会面临罚款、应用市场下架、企业纳入失信名单等处罚，且需要整改，整改完成后才可正常上线运营。

对此，百度安全部推出移动应用安全治理平台，集合应用安全加固、应用安全检测、应用隐私合规多产品，形成一套移动应用安全解决方案。

二、百度应用加固与安全检测

（一）产品介绍

百度应用加固与安全检测，是百度安全旗下一款面向智能终端应用的安全加固产品和服务，依托百度公司 20 年的安全实践和技术积累，已拥有多项安全专利和行业资质。技术能力包括但不限于代码保护、数据加密、运行时防护等数十项加固能力，可全面提高智能终端应用的安全指数，同时满足工信部及各地方监管部门的合规需求。目前，百度应用加固的产品矩阵如下，客户可根据自身业务需求，选择相应产品使用。

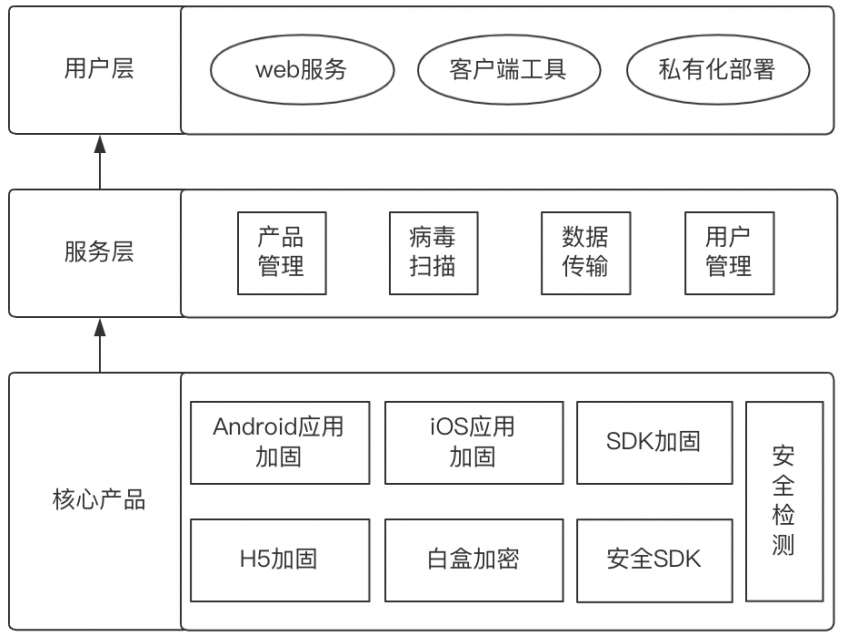
1) Android 应用加固
2) iOS 应用加固
3) Android SDK 加固
4) iOS SDK 加固

5) H5 加固

6) 白盒加密

7) 安全 SDK

8) 安全检测



1.Android 应用加固

针对目前 Android 应用存在的破解、篡改、劫持、数据泄露等各类安全风险，百度 Android 应用加固基于 VMP 的高级 SO 和 DEX 代码加固方案，高强度的资源和数据文件加密方案，可有效保护应用安全，满足客户安全和评测相关需求。

- DEX 文件保护

  通过 DEX 文件加壳、DEX 分离、DEX 代码 VMP 保护等方式，对 DEX 代码进行全面保护。

- SO 文件保护

  通过 SO 代码加壳，SO 动态混淆，SO 库防篡改等技术手段，全方位保护 SO 文件安全。

- 资源文件加密

  对应用中的资源文件进行加密保护。例如对应用 res、assets 目录中的资源文件加密压缩保护，避免资源被破解、泄露。

- 数据文件加密

  对应用中的本地文件、数据库、缓存数据等进行加密保护，避免数据文件被破

解、窃取。

- 完整性保护

  可针对关键文件、全部文件进行完整性校验，并支持签名校验和多签名验证（针对游戏联运需求）。

- 反调试、防篡改

  使用高级反调试，签名保护等技术，可以有效防止动态分析、动态注入、防 Dump，避免应用被篡改。

- 运行时防护

  提供应用运行环境检测能力，可以精准识别 ROOT、模拟器、hook、多开等环境风险因素，降低环境因素带来的安全风险。

2. iOS 应用加固

针对 iOS 应用存在的破解、篡改、劫持等各类安全风险，百度 iOS 应用加固基于源码级的安全防护方案，通过安全的源码编译，有效保护应用安全，满足客户安全和评测相关需求。

字符串加密：对程序内字符串进行加密，程序运行的时候动态解密，使黑客想要逆向定位到关键函数的难度大增。

- 字符串加密

  对程序内字符串进行加密，程序运行的时候动态解密，使黑客想要逆向定位到关键函数的难度大增。

- 代码混淆和替换

  通过函数混淆、符号混淆、代码逻辑混淆、控制流平坦化等方式，极大降低代码可读性，提升代码破解难度。

- 防篡改

  防止破解者对应用的篡改、重打包等作弊行为。

- 运行时防护

  针对应用运行环境进行检查，防越狱、反调试、防注入、防 hook。

3. Android SDK 加固

- SO 文件加固

  SO 加壳、SO Linker、SO 防调用、SO VMP 等。

- Java 代码加固

  支持 Java VMP。

- 防调用

  防止 SDK 被非授权的第三方应用集成和调用。

- AAR 包加固

  对 AAR 包采取高级虚拟化方案进行加固保护，防止 Java 代码被反编译和恶意篡改。

- JAR 包加固

  对 JAR 包内的 Java 代码进行虚拟化保护，防止 SDK 核心逻辑被逆向分析。

4. iOS SDK 加固

技术能力点与 iOS 应用加固等同。

5. H5 加固

- 多样化混淆

  变量名称混淆、控制流混淆、指令替换、混淆代码插入、代码压缩。

- 强化加密能力

  字符串加密、代码整体加密、属性加密、VMP 加密。

- 运行时防护

  反调试、运行时变形、域名锁定、禁止控制台 LOG 输出。

6. 白盒加密

- 一机一密

  采用一机一密的加密机制，最大限度保证密钥和数据安全。

- 加密算法

  支持 AES、SM4 等加密算法，融合密钥，提供安全加密方案。

- 加密强度可配置

  客户可根据业务需求、数据处理能力，配置不同的加密强度。

- 支持多种开发语言

  C/C++、Java、Python、PHP。

- 支持多种操作系统

  Android、Linux、iOS、Windows、AIoT。

7. 安全 SDK

1）安全软键盘

- 信息输入保护

  从输入前、输入时、输入后等多个维度进行数据保护。

- 随机分布式虚拟键盘

  对数据输入过程、数据存储过程、内存数据换算过程全程加密，有效避免通过键盘的使用造成信息泄露。

2）防劫持 SDK

- 视图焦点判断

  通过判断当前视图焦点的变化来感知应用界面是否被恶意程序劫持。

- 异常行为检测

  界面防劫持 SDK 帮助用户及时发现钓鱼行为，保障用户的信息安全。

3）防截屏 SDK

利用屏幕动态检测技术，防止应用界面被非法截屏、录屏，保护客户知识产权。

4）通信加密 SDK

基于百度业内首创 Mesalink 协议，面向嵌入式设备的安全通信协议栈，通过 Rust 语言实现，在语言层面最小化内存漏洞风险，保障通信安全。

8. 安全检测

为 APK、IPA、SDK 提供自动化应用检测及报告服务，报告提供风险说明及修复建议，帮助客户及时发现漏洞及风险，提高 APP 安全防护能力，依照相关法规要求进行安全检测，针对检测出的风险，可以通过应用加固保护代码和数据，保障应用符合相关法规检测规范。

- 静态检测

  以预设的安全问题特征为指导，通过静态的语法分析、控制流/数据流分析等技术，对应用的代码、配置、资源进行分析，发现潜在的安全风险

- 动态检测

  基于稳定性高、可扩展性强的硬件虚拟化技术，通过模拟真实攻击场景，检测应用对恶意攻击的防范能力

- 内容检测

  采用人工智能技术对应用内的图像、文本库进行检测，排查涉政暴恐、色情污秽等违规违法内容

- 深度检测

  自动化破解应用部分保护措施，发现深层次安全问题

（二）产品优势

1. 安全性更高

- 全数据加密保障。
- 累计服务千余家客户，拥有高稳定性，加固后零破解。
- 符合百度系产品高安全性标准规格，稳定应用于百度系各业务线。

2. 兼容性更强

- 适配市面上 TOP600 机型。

- 兼容 Android4.0 至最新版本，兼容 AAB 格式，兼容 iOS 最新版本和各类 iOS 设备。
- 加固技术能力支持 Android/iOS/Linux/Windows/MacOS 等各种操作系统。

3.性能更优越

- 加固后对平均启动时间的影响几乎为 0（小于 0.5 秒）。
- 加固后包体积增量不超过 5%，大部分 APP 可实现比加固前小。
- 4.服务更专业
- 自研自营，自身工程师及运营团队提供专业售前售后咨询服务，7*24 小时高质高效。
- 针对不同类型客户和使用场景，提供多种接入方式。
- 可提供整套 APP 安全解决方案（应用加固+漏洞扫描+隐私合规等）。

（三）应用场景

1.金融行业

金融因其行业特殊性,加之目前智能手机尤其是 Android 手机的生态环境较为开放，权限控制灵活。应用自身面临诸多风险，如：

- 窃取用户隐私信息，进行精准诈骗和恶意营销。
- 病毒、木马控制用户手机，钓鱼 APP 捕获用户账户信息，窃取、转移用户资金。
- 金融 APP 开发单位缺乏移动安全技术和解决方案，防御方式简单，易被攻破。
- 用户安全意识低，缺乏风险识别能力，给不法分子可趁之机。

百度应用加固解决方案可为银行、证券、保险、互联网金融等行业 APP 提供全方位的加固保护，保障 APP 主体和用户利益。

2.教育行业

基于移动互联网的发展，教育行业逐渐由线下模式拓展到线上，通过网站、APP 等线上平台进行教育培训。线上教育要求对本地文件、数据库、缓存数据等进行加密保护，避免数据文件被破解，且数据保护的安全等级要求高，一旦发生线上安全事故，将会造成较大范围的恶劣影响。

百度应用加固解决方案基于全数据加密保障，为各类教育类 APP 提供全方位的文件保护和数据保护，且能满足 APP 的监管上线需求，上线后 APP 持续运营无影响。

3.政企行业

随着移动互联网的发展，政府信息化建设已经从传统的 PC 端转移到移动端，以移动办公、移动执法、移动审批、移动巡检等为代表的移动信息化已成为政府部门履行自身职能的必备工具，越来越多的政企用户开始依赖移动 APP 展开工作及相关业务。对于政企

行业，移动信息化的发展规划需要综合考虑安全风险及合规风险。

百度应用加固解决方案致力于为运营商、交通、政务平台、大型企业等政企行业，提供 APP 防篡改和二次打包、数据加密保护等多项安全技术能力，保障业务的顺利开展和企业的正常运作。

4. IoT 行业

IoT 行业范围包括但不限于智能汽车、智能电视、智能音箱、智能穿戴、机器人等设备品类，因 IoT 设备终端和系统碎片化严重，极易成为黑客攻击的对象，具体表现为：

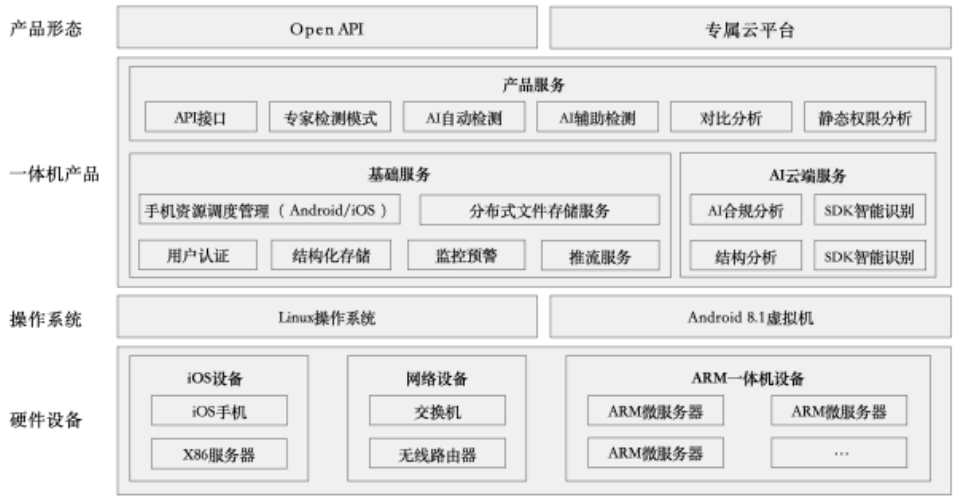
- 恶意操作/控制：物联网应用程序/设备容易受到恶意代码攻击、绕过控制、篡改数据的完整性
- 信息泄露/窃取：物联网应用程序/设备可能泄露用户的私人资料、账号、密码、交易凭证等信息
- 知识产权窃取/盗版：没有受到保护的物联网应用程序/设备，将会暴露嵌入式设备专有算法，被窃取知识产权并生产相应盗版产品
- 未知漏洞利用/曝光：物联网设备会产生各种未知的漏洞，这些漏洞的曝光会吸引大量的黑客对相关设备的攻击
- 安全模块破解：通过各种攻击手段破解、绕过物联网设备软硬件的安全防护措施

百度应用加固解决方案，基于自身的加固能力，以及在小度智能音箱、自动驾驶等业务上的经验积累，可为各类 IoT 智能设备提供定制化的加固解决方案，满足 IoT 设备的安全需求和客户业务场景需要。

三、史宾格安全及隐私合规平台

（一）产品介绍

史宾格安全及隐私合规平台是业界首款对外提供服务的 APP 收集使用个人信息合规风险检测和治理系统。基于 AI 检测技术，深度挖掘 APP 隐私合规风险产生的源头，包含 APP 权限过度申请与使用多种维度。并依据《中华人民共和国网络安全法》《信息安全技术个人信息规范》《APP 违法违规收集使用个人信息自评估指南》等国家法律法规，生成可视化的隐私合规情况检测报告。协助监管部门高效、精准地发现 APP 合规问题，帮助企业高效、低成本地开展 APP 合规问题自查，满足监管要求。



（二）产品核心功能

史宾格安全及隐私合规平台具备完善的应用隐私风险检测与技术实践能力，拥有市场最全的第三方 SDK 隐私检测能力和特征库，以及权限到 API 的映射关系数据库，保障应用隐私风险检测的专业性和全面性，从而促进应用隐私合规。

1. APP 与 SDK 静态权限分析

上传 APK \ SDK 即时检测敏感权限的申请和使用情况，及时发现过度申请权限、冗余权限与代码，及使用不合理的敏感权限等问题，判断敏感权限使用的合理性。史宾格会按照涉及个人信息的敏感级别将敏感权限分为高敏、中敏和低敏权限 3 个等级，并精准定位发生敏感权限使用的代码位置，并可视化地展示出来。对于集成了三方 SDK 的 APP 而言，对于其集成的三方 SDK 我们也可实现自动化检测，轻松解决第三方 SDK 的权限使用不可控的难题。

将 APP 中权限的使用场景划分为自身 APP 使用、SDK 使用和其他使用，并实现精确定位到代码的位置可视化展示代码分布。

2. APP 动态场景检测

动态场景检测提供了对 APP 的隐私政策的合规性检测能力，以及在不同运行环境下敏感权限的申请告知场景和使用场景的检测能力，是判断 APP 隐私合规的重要依据。史宾格安全及隐私合规平台通过云端手机模拟 APP 的真实使用环境，包括前台使用场景、Home 后台场景、Back 后台场景、锁屏场景、解锁场景、通讯场景、设备重启场景等。在动态的模拟使用过程中，对隐私政策文本及 APP 的隐私行为进行检测和分析，最终生成可视化的隐私合规检测报告。

为了解决敏感权限下个人信息的行为溯源问题，在动态检测场景下，对于敏感权限可以查看在不同触发场景中调用代码的触发堆栈，统计触发次数并对触发场景截图，使

敏感权限的个人信息采集行为有缘可溯。

数据传输分析实现对 APP 传输采集的个人信息的检测，可以检测出 APP 向哪些域名传输个人信息，以及是否存在跨境传输等情况，使个人信息的传输流向更加透明清晰，及时发现信息传输的潜在隐私风险。

同时，专家模式提供个人信息收集类型、第三方 SDK、产品隐私设计完整度、权限使用行为、数据安全等多重维度的合规性检测能力，以及在不同运行环境下自动化识别产生的违规收集行为，深入发现 APP 隐私风险行为，并基于 VPNService 技术的应用流量监控方案，自动分析出 APP 在网络数据传输过程中是否上传了个人敏感信息，并实现定位到具体的服务。

为了让客户更便捷地发现隐私合规风险，我们的隐私合规检测报告以政府发布的规范为标准进行标准化输出，APP 隐私合规问题清晰可寻。

3.APP 收集使用个人信息合规性检测

APP 收集使用个人信息合规性检测是基于 AI 静动态检测能力及智能语义分析技术，并以国家发布的规范或标准为依据，对 APP 个人信息采集行为进行逐条对应分析，判断数据采集行为的合规性，通过具有针对性的自动化检测方式，快速完成复杂的检测流程，即时生成精确的合规性检测报告。

史宾格安全及隐私合规平台的合规性检测可实现自动化动态生成检测报告，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，以国家规范为检测依据，为客户实现有据可依，针对于存在风险的隐私行为进行逐条对应，使违反的法规条目更加清晰明了，并可根据对应的整改建议优化产品提升效率。

4.安全服务

为了应对 APP 存在的主流安全风险，史宾格安全及隐私合规平台为 APP 提供病毒误报检测和漏洞检测等安全服务。基于强大的多引擎安全检测系统，检测 APP 是否会在市场主流的反病毒软件报毒，以便安全上架。基于强大的漏洞检测引擎，提供 APP 漏洞检测的安全服务，使 APP 提前发现所存着的潜伏风险避免造成重大损失。

5.权限管理

为了满足不同类型的客户对业务数据安全保护需求，史宾格安全及隐私合规平台提供了完整的权限管理体系，支持多角色设置，从多个维度保护数据安全。针对平台层级的管理需求，可设置平台级管理员，对平台的业务和业务成员进行管理；针对业务层级的管理需求，可设置业务管理员，对单个业务的 APP 和成员进行管理。各业务之间数据互相隔离，以保证专人做专事，确保数据在有限的范围内可见，从而有效保护业务数据安全。

6.多版本对比

通过对产品多个不同版本之间的敏感权限申请和使用情况的对比，帮助产品快速定

位隐私合规问题起始版本和原因，更快解决隐私合规问题。

（三）产品优势

1.领先的 AI 检测技术

依托于百度对技术研发的巨大投入，以先进的人工智能技术为支撑，覆盖了产品设计、开发测试、上线前安全测试和上线后安全监控等 APP 全生命周期的隐私合规需求。包含隐私数据采集、权限使用场景、 隐私政策管理等多重纬度的深度检测能力。

2.高效的自动化检测

基于百度云手机集群的 AI 全自动化隐私风险发现与检测能力，提供隐私专项检测、隐私合规检测、权限分析、专家模式等服务。深度挖掘隐私合规风险点、快速处理大批量App，替代人工翻查代码，降低时间与人力成本，显著提升检测效率。

3.深度对齐监管标准

专业的法务团队紧跟国家政策法规，实现检测结果深度对齐《App 违法违规收集使用个人信息行为认定方法》、工信部 337 号文及 164 号文、《个人信息安全规范》(GB/T 35273)等规范性文件、国家标准，对 APP 收集使用用户个人信息的行为进行逐条对应分析。

4.高级定制化开发

可基于企业用户场景需求，对系统及功能模块进行定制开发，并集成至自己的业务平台内，低于对数据安全与稳定性有要求的企业来说是非常好的选择，并可支持客户个性化业务需求的自由扩展，以满足不同业务需求。

5.全面支撑监管治理

经过长期的实践与广泛应用，凭借发现 APP 违规收集使用个人信息的自动化检测能力，已先后与工信部信通院、黑龙江网信办获等多家监管部门及下属单位达成技术合作。为其提供 APP 隐私违规检测技术支撑，全面支持监管部门在 APP 违规收集个人信息专项治理、建立联动监管平台方面的具体工作。

6.资深专家团队服务

深耕隐私合规领域，凝聚百度隐私合规法务团队与百度安全管理团队的智慧与经验。由资深安全专家与法务精英，共同为您提供包含法务咨询、安全专家解读等合规辅导的增值服务。

（四）应用场景

1.开发者应用场景

当 APP 开发人员流动较大或开发人员众多时可能导致代码追溯困难，监管机制不健全或测试流程不完善可能导致隐私问题得不到重视，业务人员对法律法规理解不深入可

能导致隐私风险难以发现等困难。应用开发者自身的研发成本和精力有限，传统的人工手动翻查代码的方式费时耗力，却很难精准找到问题代码的具体位置，从而导致应用隐私风险问题无法彻底根查，更无法实现治理。

史宾格安全及隐私合规平台可以帮助开发者自动化地检测出自己的 APP 的敏感权限申请和使用的宏观状况，精准定位问题代码位置和问题场景，帮助开发者在 APP 上架前进行隐私合规自测，合规后再上架应用市场，避免出现舆论或合规风险。

- 自动化检测，极速发现隐私合规风险
- 快速定位问题代码所在位置，哪怕是集成的三方 SDK 违规使用敏感权限也可轻松查出
- APP 上架前强制检测，坚决不让有问题的包流向市场
- 对个人信息传输进行流量监控，快速发现个人信息流向的传输风险
- 提供 APP 的多引擎病毒误报检测和强大的漏洞检测能力，以便 APP 安全上架

2.大型企业应用场景

提升产品隐私安全、保障用户信息安全、降低企业法务及舆论风险已经成为当今企业热点关注话题。当企业对旗下的产品矩阵进行综合的隐私合规监控和管理时，缺乏对标监管的标准、APP 隐私风险检测效率低、检测结果不够准确，第三方 SDK 隐私问题不可控，隐私合规落实困难，成为企业隐私安全治理面临的重要问题。

史宾格安全及隐私合规平台从敏感权限检测，动态场景检测，到企业 APP 的隐私风险监控，一站式解决企业 APP 矩阵隐私风险治理问题，为企业的良好口碑和健康发展提供更好的保障。

- 检测标准化：检测标准对标国家监管标准，包括隐私数据采集、权限使用场景、隐私政策合规检测等多维服务；
- 企业级治理平台：帮助企业高效监控和治理业务隐私合规风险。

3.应用市场应用场景

应用市场作为 APP 在市场的传播者与市场的管理者，对平台内发布的 APP 负有隐私合规检测的责任和义务，需要对每天上架的应用进行批量的隐私政策合规检测及敏感数据收集检测，以尽监管义务。但目前市场上缺乏自动化的隐私合规检测工具，应用市场难以对隐私风险做集中监控与治理。

史宾格安全及隐私合规平台可以为应用市场提供定制化的检测接口，与应用市场控制端形成无缝衔接，帮助应用市场在不破坏原有运营框架的情况下，精准批量地对应用市场内发布的 APP 进行隐私合规检测。

- 自动化检测：通过接口调用的方式自动化完成检测
- 标准化检测：检测标准对标国家监管标准
- 批量解决：通过接口调用的方式满足高并发量的检测需求

4.监管机构应用场景

随着《信息安全技术个人信息安全规范》的正式生效，中央网信办、工业和信息化部、公安部、市场监管总局联合开展“APP 违法违规收集使用个人信息专项治理”活动，各监管机构纷纷响应 APP 专项治理，开展 APP 隐私风险检测已初具规模，但是目前检测技术方法、效率还有待优化和提高。

鉴于此，百度安全提供自动化的隐私风险检测工具“史宾格安全及隐私合规平台”，可以达到标准化检测，替代传统的人工筛查，解决人工筛查工作中的标准不一致、漏检率高等问题。真正做到批量检测、高效输出、准确定位，帮助监管层迅速发现 APP 中的隐私风险问题，最大化降低人力及时间投入成本。

- 检测高效：可扩展的自动化检测，能够快速处理大批量的 APP，满足监管机构大量检测的业务需求。
- 检测准确：静态与动态有机结合，运用沙箱技术对 APP 的隐私采集和使用行为进行深入的分析，得出精确的结果。
- 以国家规范为依据，提供个人信息收集及使用合规性检测，对违反法规的隐私风险行为进行逐条对应，隐私合规问题一目了然，并针对检测出现的个人信息安全问题，提供合理的整改建议，无需过多人工干预和复杂的检测流程即可得到规范的可视化检测报告。