爱加密
www.ijiami.cn

疫情之下的爱加密远程移动办公信息安全思路

北京智游网安科技有限公司

2020年2月

爱加密
www.ijiami.cn

目 录

CONTENTS

爱加密
www.ijiami.cn

01
公司介绍

公司介绍

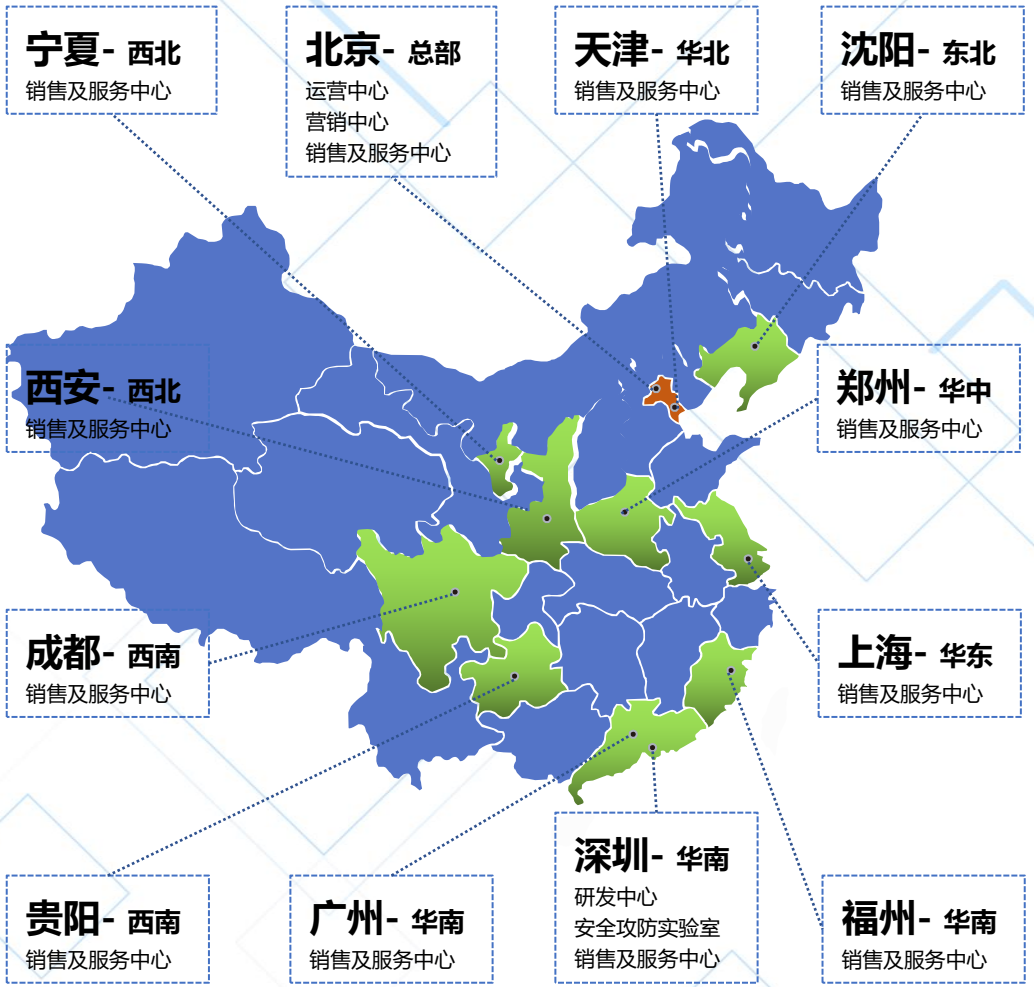
爱加密成立于2013年，是国内知名的移动信息安全综合服务提供商。拥有安全防护、安全检测、安全管理、业务运营、威胁感知、安全监管、安全服务七大产品体系，是为移动应用提供全生命周期安全服务的移动信息安全品牌。爱加密至今共服务移动应用100万+，监控互联网应用1500万+，服务行业客户覆盖政府、运营商、金融、游戏、教育等多个行业。

行业用户服务
2000+

市场保护APP
100万+

网络监测APP
1500万+

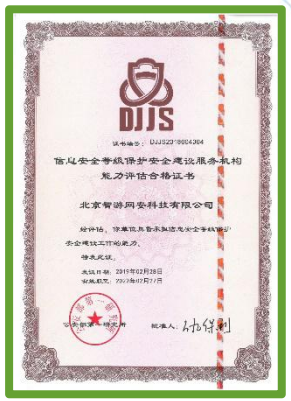
智能终端设备
10亿+

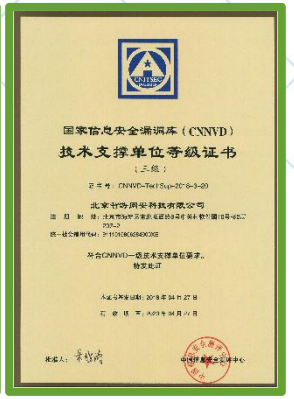


公司介绍——企业资质

爱加密 www.ijiami.cn

- 信息安全等级保护安全建设服务机构能力评估合格证书
- 通信网络安全服务能力评定证书 风险评估一级
- 通信网络安全服务能力评定证书 网络安全设计与集成一级
- CCRC信息安全服务资质认证证书:信息安全风险评估服务资质（一级）
- CCRC信息安全服务资质认证证书:软件安全开发服务资质（二级）
- CCRC信息安全服务资质认证证书:信息系统安全集成服务资质（二级）
- CCRC信息安全服务资质认证证书:信息系统安全运维服务资质（三级）
- CCRC信息安全服务资质认证证书:信息安全应急处理服务资质（三级）
- ISO9001质量管理体系认证证书
- ISO20000信息技术服务管理体系认证证书
- ISO27001信息安全管理体系认证证书
- 软件企业认定证书
- 信用等级（AAA）评价证书
- CMMI3级资质证书
- 国家高新技术企业/中关村高新技术企业
- 国家信息安全漏洞库技术漏洞支撑单位（CNNVD）三级
- 商用密码产品生产定点单位
- 国家计算机病毒应急处理中心优秀技术支持单位
- 网络安全应急服务支撑单位证书





公司介绍——软件著作权（70项+）

爱加密 www.ijiami.cn

部分著作权证书展示

- 智游网安爱加密防反编译软件V3.0
- 智游网安爱加密防二次打包软件V3.0
- 智游网安爱加密防动态调试注入软件V3.0
- 智游网安爱加密本地存储数据加密软件V3.0
- 智游网安爱加密安全键盘软件V3.0
- 智爱加密移动应用安全软键盘-ios V3.5.0
- 移动应用监管平台V1.0
- 爱加密iBOX智能操作系统V2.0.0
- 爱加密移动应用安全综合实训平台V2.0

公司介绍——典型客户

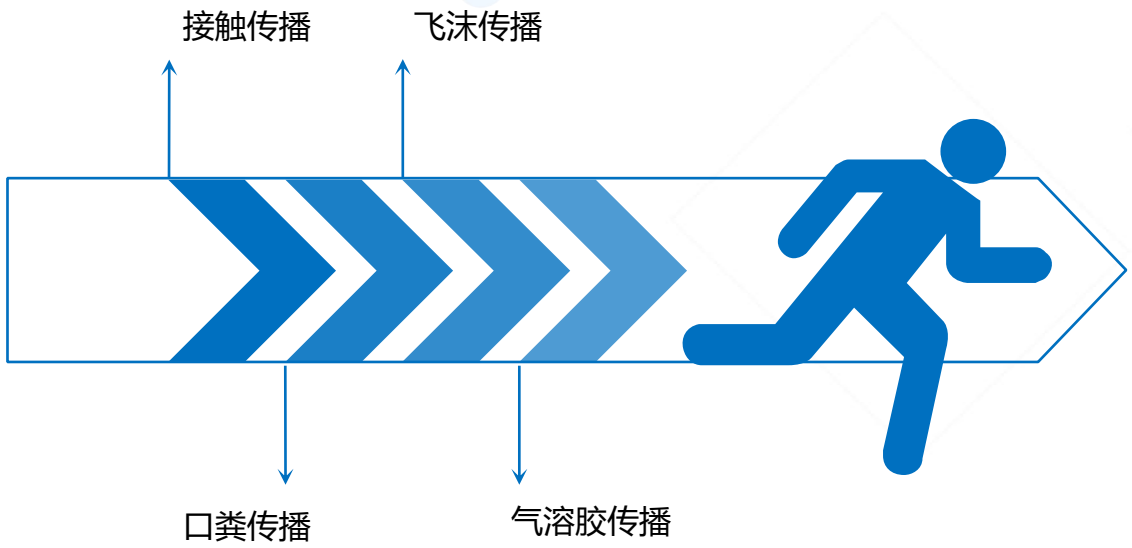
爱加密 www.ijiami.cn

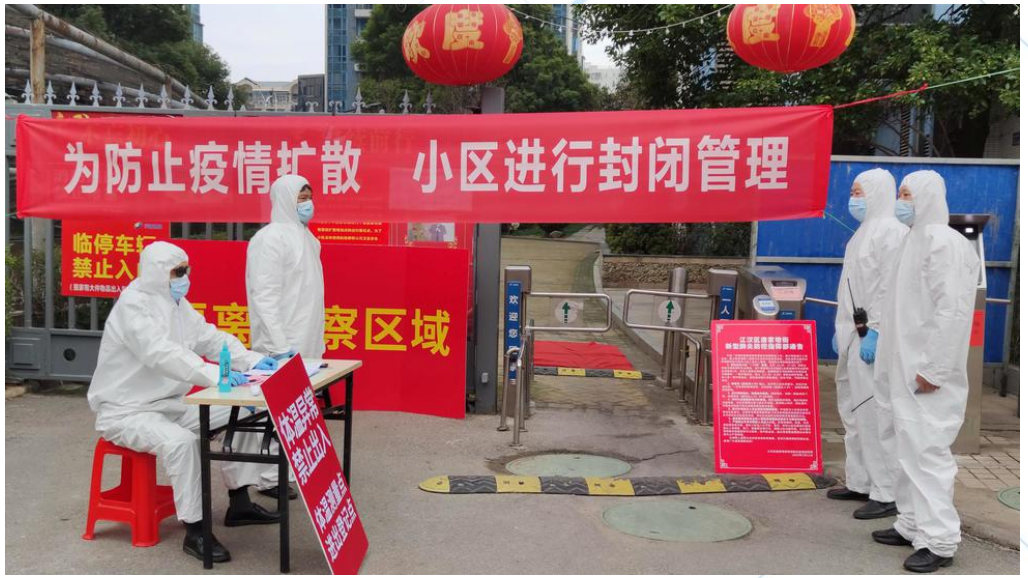
02
背景介绍

封闭管理

- **武汉市新型冠状病毒感染的肺炎疫情防控指挥部通告**

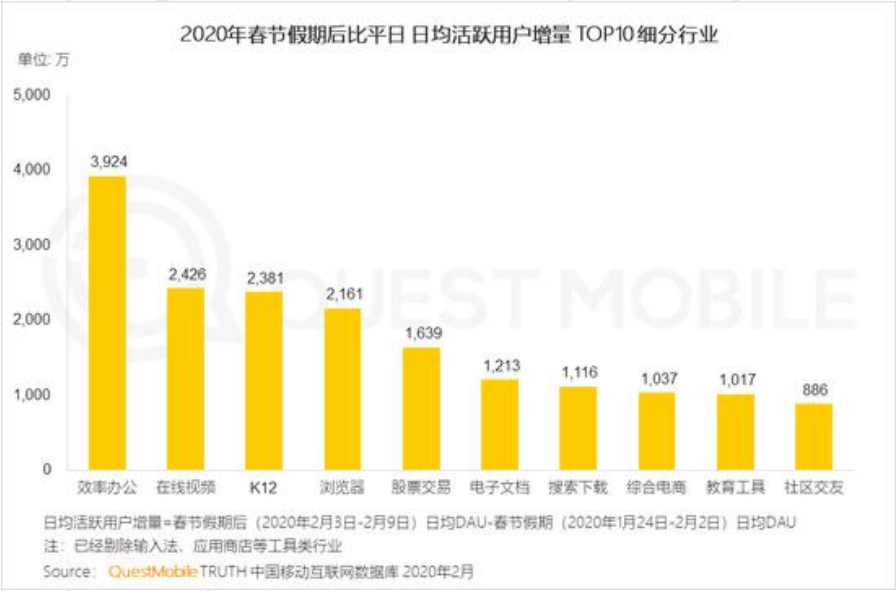
1月23日凌晨，武汉市新型冠状病毒感染的肺炎疫情防控指挥部发布消息，为全力做好新型冠状病毒感染的肺炎疫情防控工作，有效切断病毒传播途径，坚决遏制疫情蔓延势头，确保人民群众生命安全和身体健康，自1月23日10时起，武汉全市城市公交、地铁、轮渡、长途客运暂停运营；无特殊原因，市民不要离开武汉；机场、火车站离汉通道暂时关闭





移动应用APP活跃

名称	现价	涨跌幅↓
US 跟谁学 GSX	44.98	18.81%
US 有道 DAO	25.40	14.31%
US 无忧英语(51 COE	22.52	10.39%
US 好未来 TAL	59.40	2.48%
US 新东方 EDU	141.76	2.01%



某医疗类APP累计访问人次达11.1亿，APP新注册用户量增长10倍，APP新增用户日均问诊量是平时的9倍

在线教育类股价暴涨，某教育APP平均日活同比增幅和新增用户同比增幅分别为834.31%和2422.66%

春节后一周，远程办公和在线学习的需求明显上升，效率办公领域日均活跃用户规模上涨近4000万、K12上涨过2000万

安全风险

爱加密
www.ijiami.cn

03
解决方案介绍

远程移动办公安全解决方案

爱加密
www.ijiami.cn

身份管理

设备管理

应用管理

运维管理

安全评估

安全加固

安全监测

爱加密
www.ijiami.cn

A

安全维度

1、安全评估

2、安全加固

3、安全监测

安全评估——源码安全审计

源代码审计服务的范围包括使用Java、Html、PHP、Python、JavaScript等主流语言开发的B/S应用系统、使用C、C++、Java等主流语言开发的C/S应用系统，以及使用XML语言编写的文件、SQL语言和数据库存储过程等。

移动应用端：主要包括Android、Java、JavaScript、Xml、Html、Sql

Web端：主要包括Java、PHP、Python、C++、C、JavaScript、Xml、Html、Sql

安全评估——自动安全检测

爱加密 www.ijiami.cn

检测项

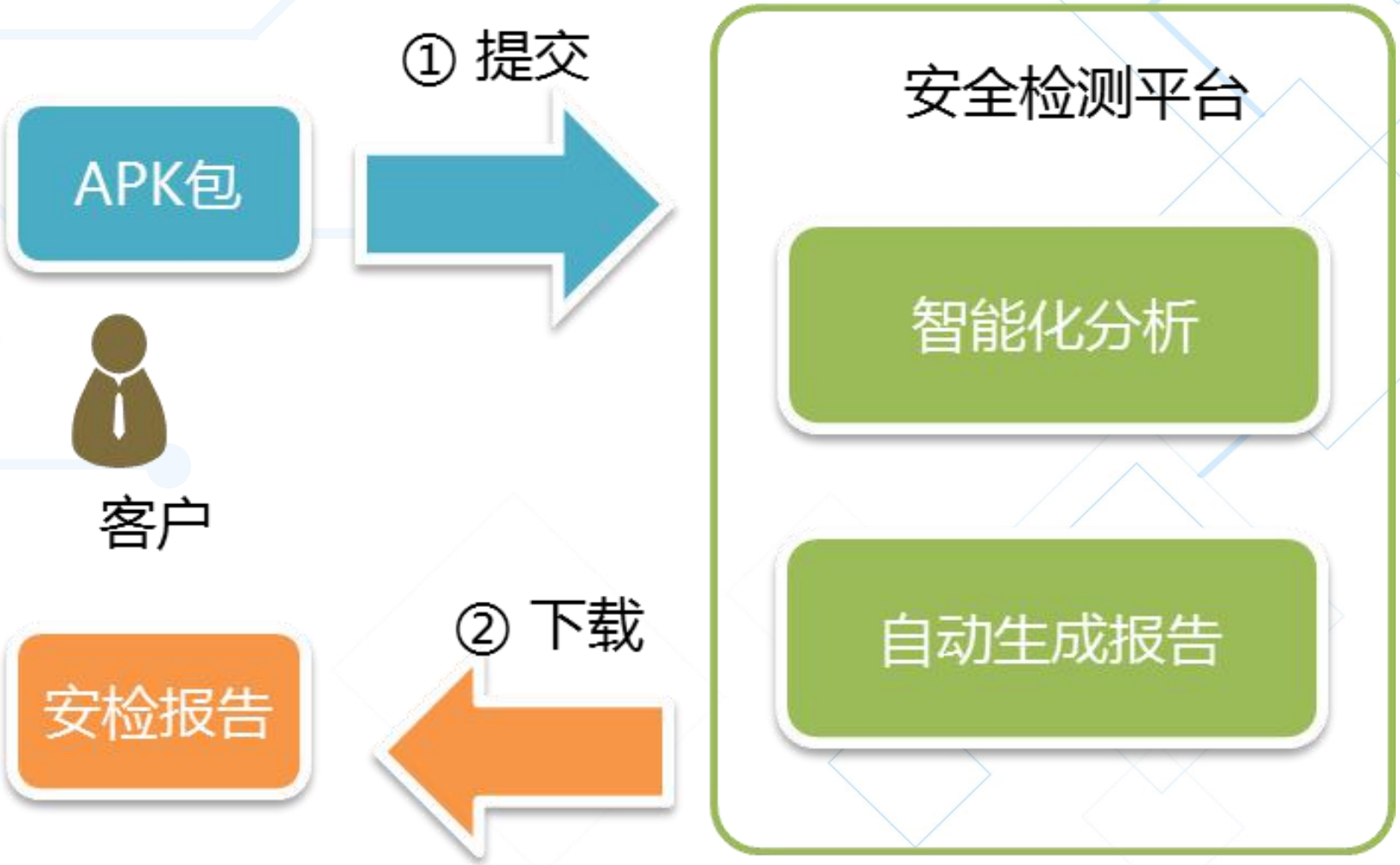
Android：75项

IOS：29项

SDK：29项

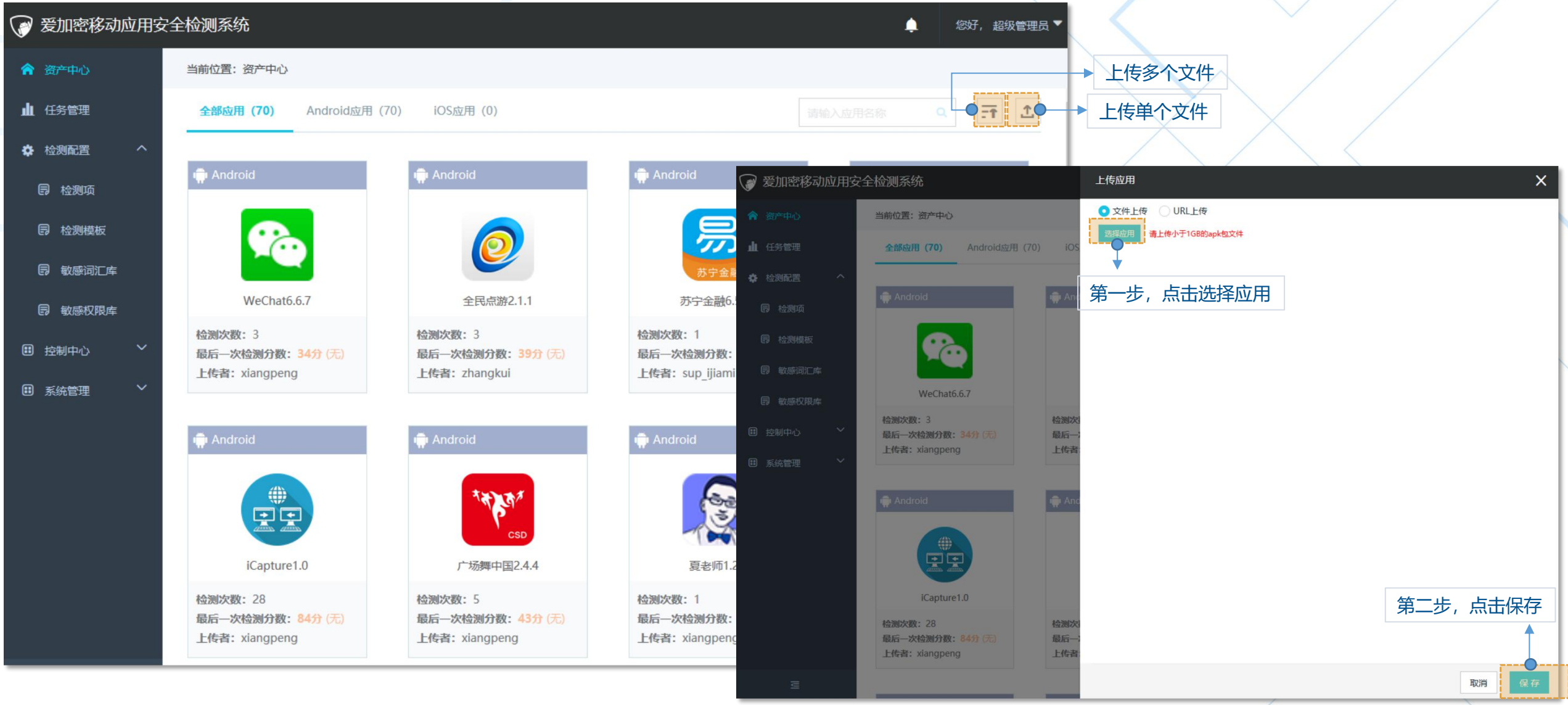
公众号：21项

安全评估——自动安全检测流程



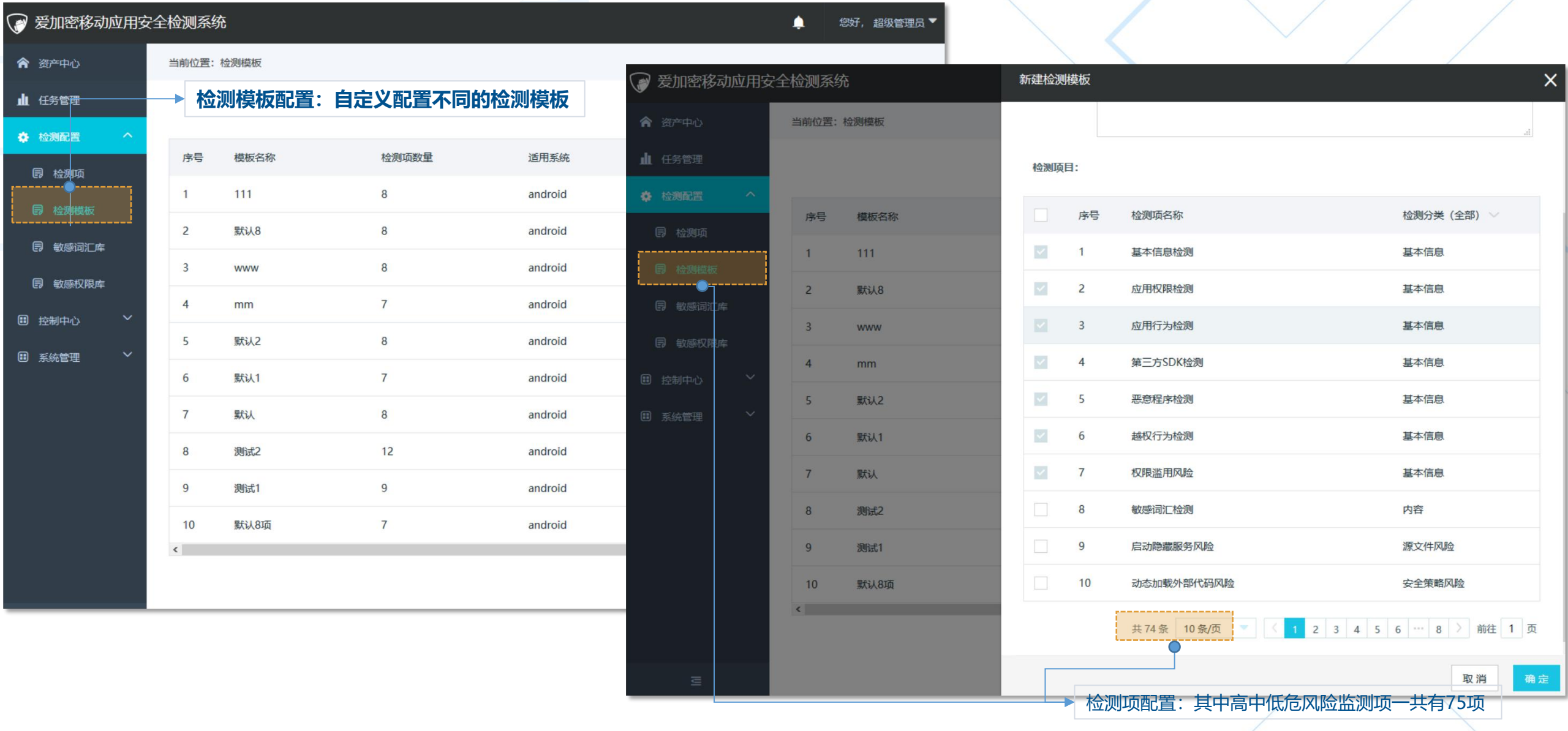
安全评估——自动安全检测

爱加密 www.ijiami.cn



安全评估——自动安全检测

爱加密 www.ijiami.cn



安全评估——自动安全检测

安全检测评估报告

XXXX

爱加密
www.ijiami.cn

移动应用安全评估平台

http://www.ijiami.cn/safetyAssess

文件状态：	公司名称：	深圳爱加密科技有限公司	文档名称：	安全检测评估报告
【√】正式发稿	检测时间：	2016-08-08	密级：	中

7	敏感行为检测	低危
8	敏感函数检测	安全
9	敏感词汇检测	低危
10	动态加载 DEX 行为检测	低危
11	代码混淆检测	安全
12	DEX 保护检测	高危
13	DEX 加花保护检测	中危
14	SO 保护检测	安全
15	应用完整性检测	安全
16	程序签名保护检测	安全
17	动态调试攻击检测	安全

3.3.1.2 DEX 保护检测

检测目的	检测 APK 程序中 DEX 文件是否受保护
重要等级	高
危害	DEX 未进行保护会被攻击者通过 baksmali/apktool/dex2jar 等反编译工具逆向出代码，造成核心代码逻辑泄露、重要数据加密代码逻辑泄露等等。
检测结果	高危
检测详情	总共检测的核心关键类文件数量【253】个； 检测到未保护的核心关键类文件数量【247】个； 检测到已做保护的核心类文件数量【6】个； 检测未做保护的核心关键类文件为： 类： smali/com/transfar/tradedriver/common/ui/StartupActivity.smali 相关函数取样：... 此处省略若干函数....method public constructor <init>()V .registers 1 .prologue .line 32 invoke-direct {p0}, Lcom/transfar/tradedriver/base/BaseActivity;-><init>()V return-void

安全评估——个人信息合规评估

爱加密 www.ijiami.cn

应用APK

移动应用APK

移动应用URL

各类检测引擎

1.静态检测引擎

2.权限检测引擎

3.动态检测引擎

4.隐私检测引擎

5.内容检测（录屏）

个人信息安全知识库

行业最小权限知识库

SDK权限与行为知识库

网络行为分析知识库

行为权限对照知识库

个人信息安全检测报告

基础信息

SDK信息
（SDK名称、厂家、权限、收集信息、行为等）

APP行为分析
（行为名称、函数、函数位置、行为截图等）

个人信息安全合规性

信息（境外）传输风险

隐私条款合规性

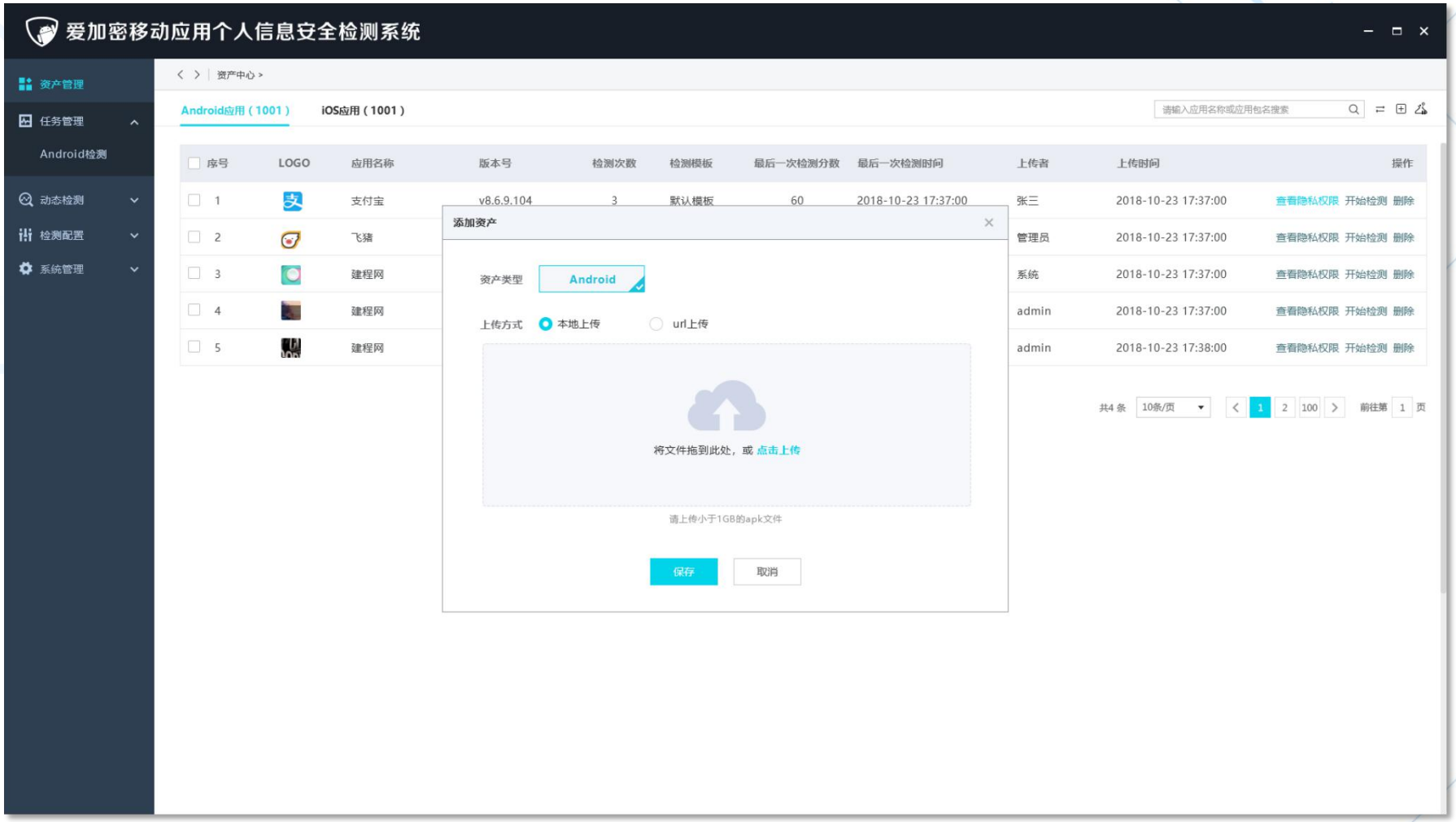
个人信息安全检测平台

移动应用大数据平台

安全维度——个人信息合规评估

爱加密 www.ijiami.cn

上传移动应用



安全评估——个人信息合规评估

检测报告

安全评估——渗透测试

爱加密 www.ijiami.cn

- **渗透测试服务**

  爱加密渗透测试服务包括了：**应用系统全量渗透测试服务、业务接口渗透测试服务。**

  - **应用系统全量渗透测试服务**
    - Android全量渗透测试服务
    - iOS全量渗透测试服务
    - 微信公众号渗透测试服务
    - Web应用渗透测试服务
    - SDK渗透测试-Android
    - SDK渗透测试-iOS

    全量渗透：对系统的安全性作全方位深入的探测发现系统脆弱的环节的过程

  - **业务接口渗透测试服务**
    - 移动业务接口安全设计风险评估服务
    - 移动业务接口渗透测试服务

    业务渗透： 对系统深层次的业务逻辑漏洞进行探测，对业务系统做更深层次、更专业的安全检查。

交付物： 1、渗透测试报告
2、渗透测试复测报告

安全加固——Android加固

爱加密 www.ijiami.cn

静态层面

防逆向

DEX文件保护
- 多DEX加固
- DEX加壳
- DEX函数分离
- DEX VMP

SO文件保护
- SO文件加壳
- SO文件高级混淆（LLVM编译级）
- ELF VMP

SDK保护
- JAR加固
- AAR加固
- SO文件保护

其它
- JS
- H5

防篡改

代码防篡改
- DEX文件防篡改
- SO库文件防篡改
- H5代码防篡改

资源文件防篡改
- Res资源防篡改
- AndroidManifest配置文件防篡改
- Asset资源防篡改

签名保护

动态层面

防调试
- 防动态调试
- 防进程调试
- 防内存代码注入
- 防内存DUMP
- 防模拟器
- 防HOOK攻击

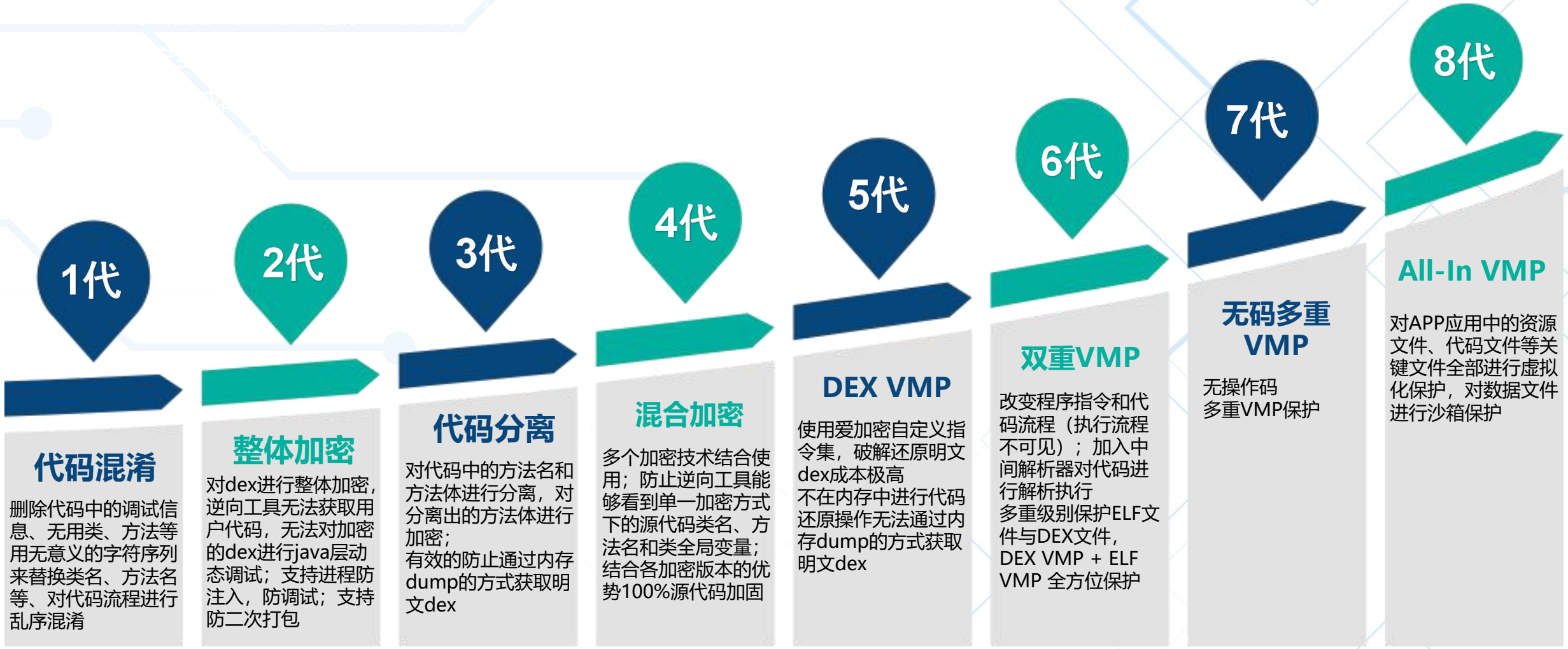
数据层面

数据防泄漏
- 内存数据
- 日志数据
- 本地数据
- 数据传输 SDK

页面数据保护
- 应用防截屏
- 应用防劫持
- 安全键盘 SDK

安全加固——Android加固发展路线

爱加密 www.ijiami.cn



安全加固——IOS应用加固

爱加密 www.ijiami.cn

安全键盘SDK

- ✓ 键盘字符混排
- ✓ 输入无回显
- ✓ 输入数据加密
- ✓ 自定义键盘视图
- ✓ 个性化设置

安全防护SDK

- ✓ 越狱检测
- ✓ 重签名检测
- ✓ Cydia Substrate框架检测
- ✓ 逆向工具检测
- ✓ 代码注入框架检测
- ✓ 调试器检测
- ✓ 反调试器检测
- ✓ 发布渠道检测
- ✓ 代码段验证
- ✓ 网络代理检测
- ✓ airplay录屏和系统截屏录屏通知
- ✓ 后台开启模糊效果

高级混淆插件

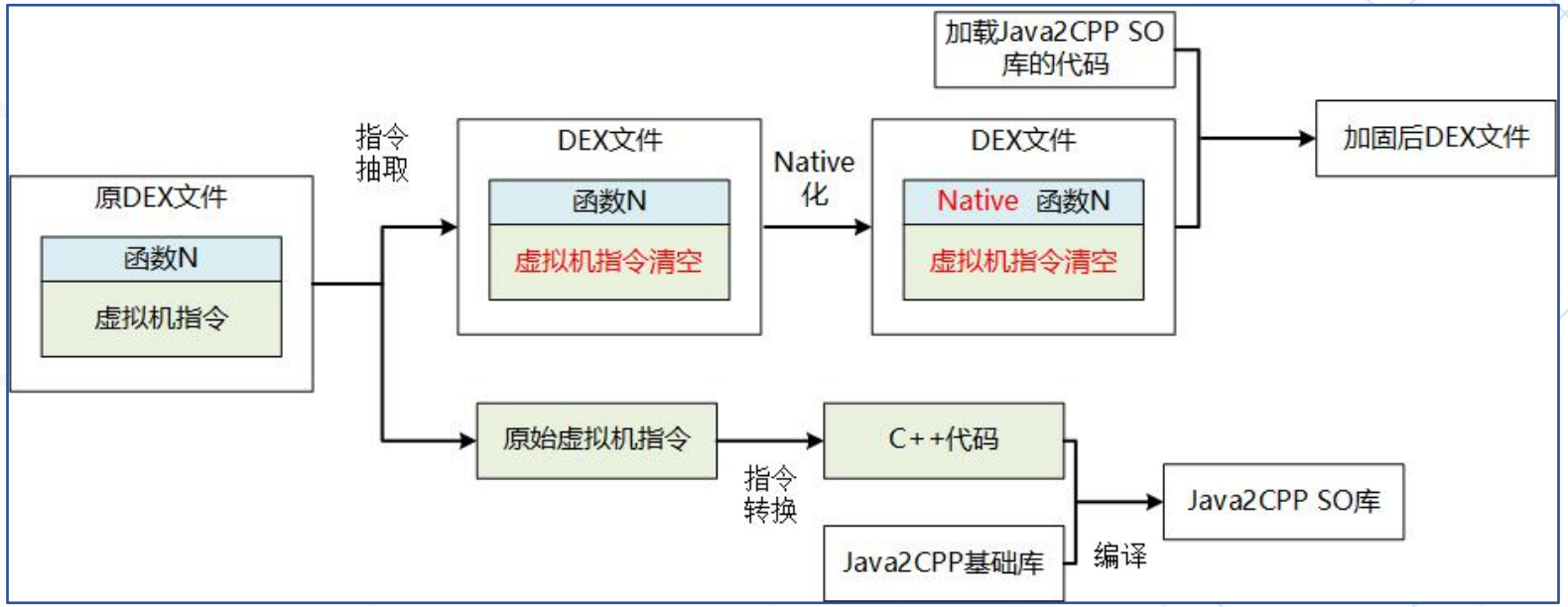
- ✓字符串加密
- ✓等效指令替换
- ✓基本块分裂
- ✓基本块调度
- ✓虚假控制流
- ✓控制流扁平化
- ✓控制流间接化

通信协议加密SDK

- ✓数据加密
- ✓文件加密
- ✓一次一密
- ✓密钥与算法融合

安全加固——JAVA2CPP

将DEX文件中的Java代码转换成C++代码，并将C++代码编译成动态库，能有效的防止破解者通过动态调试的方式获取DEX代码。java2cpp也可称为无操作码保护。



安全性高：APK经过爱加密Java2CPP安全加固技术加固后，在运行过程中不存在二代和三代加固技术会在内存中出现的整体或者部分函数还原；Native层面还原为Java层面的这个过程是不可逆的，不存在还原

性能更优：C++的运行效率比Java的高很多（10-30倍）。因为C++是属于编译型的，直接将源码编译成机器代码；Java则是解释型的，源码被编译成二进制伪代码，由Java虚拟机解释执行

安全加固——安全键盘SDK（安卓&IOS）

爱加密 www.ijiami.cn

黑客通过对系统输入法的攻击，达到对支付应用内部输入框数据的窃取。

爱加密提供“爱加虚拟键盘SDK”，用户根据开发帮助文档进行开发，该SDK有效防止键盘被非法程序进行监听后获取账号密码等隐私信息。

- 键盘字符混排
- 键盘防劫持
- 键盘防截屏
- 输入时，输入框无短暂明文显示

安全加固——安全键盘SDK（H5）

爱加密 www.ijiami.cn

全平台支持

数据加密

PC端禁用外接输入键盘

PC端不使用缓存信息

键盘抽象随机

Android端防Activity导出与界面劫持

Android端防止界面截图

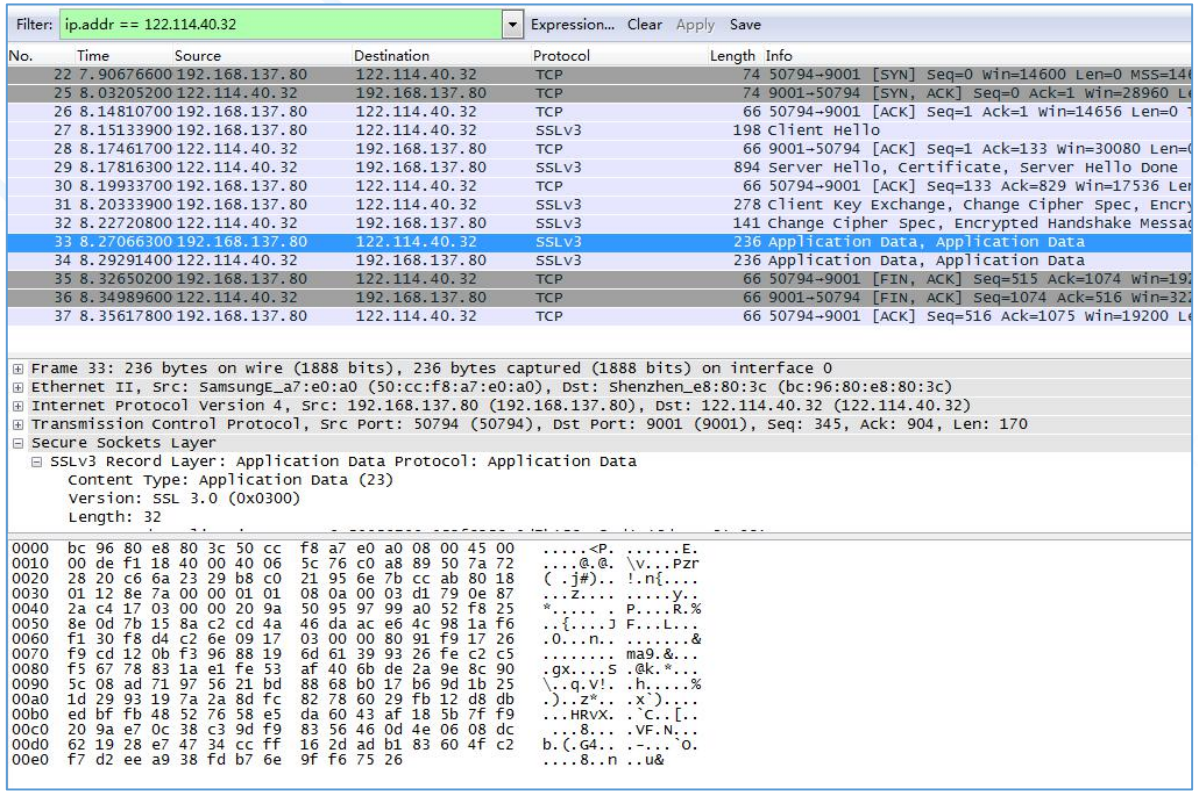
微信端防止界面截图

支持PC、Android、iOS、微信公众号、微信小程序

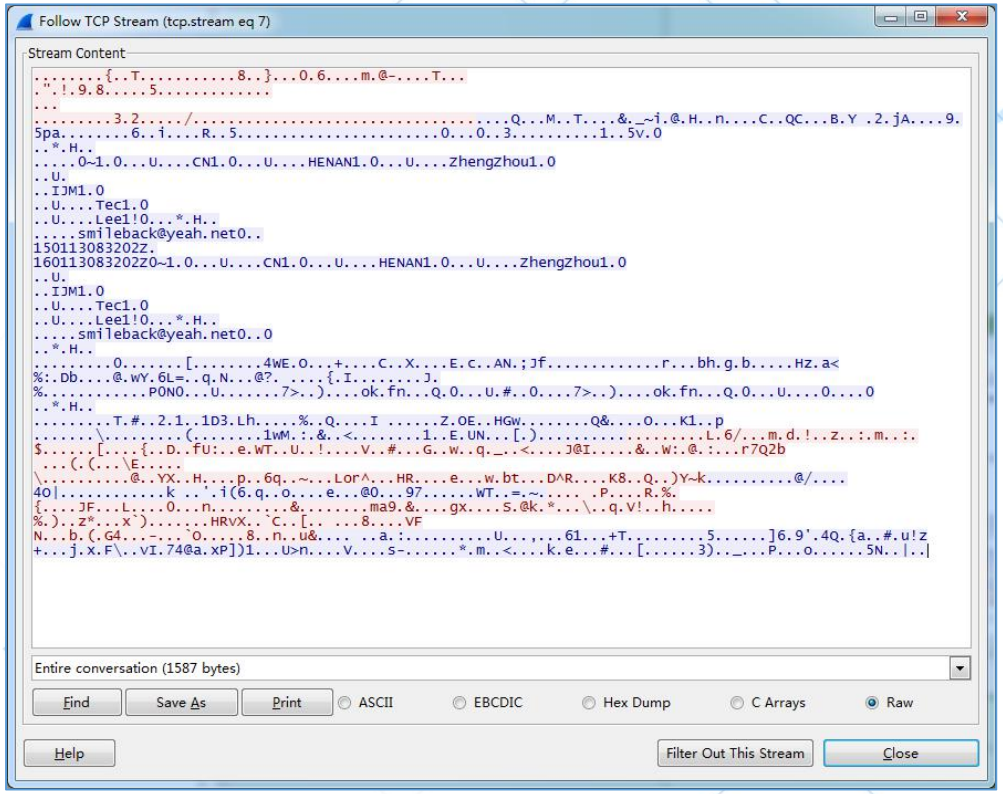
安全加固——协议加密SDK

爱加密 www.ijiami.cn

- 原理：经过数据传输加密后，抓包工具在数据传输链路中，将截获不到明文信息
- 效果：截获的数据包和数据交互信息都是加密的



加密前



加密后

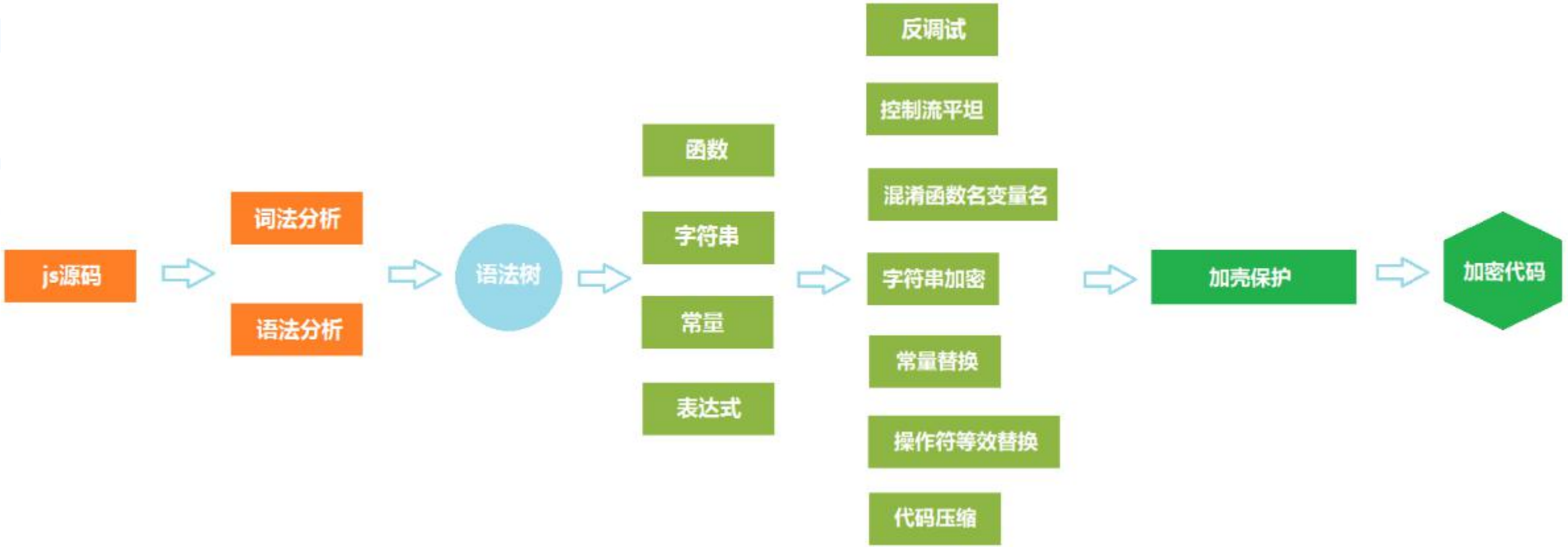
安全加固——协议加密SDK

- 本地存储的数据、文件加解密
- 网络传输的数据、文件加解密
- 支持AES和SM4算法
- 支持常规模式、一次一密模式、单向加解密模式
- 客户端支持Android、iOS、浏览器JS 、微信小程序
- 服务端支持Java、C#、Python、PHP、Nodejs

安全加固——H5加固

爱加密 www.ijiami.cn

JS控制流扁平化 | JS字符串加密 | JS数字加密 | JS代码压缩 | JS函数名、变量名混淆 | JS域名绑定检测 | JS反调试检测



1、系统自动对H5文件加密。2、系统自动对H5文件压缩与混淆。3、系统支持批量上传及下载H5文件。

安全加固——SDK加固

爱加密 www.ijiami.cn

Android SDK（Jar和AAR)

- ✓ Java代码加壳
- ✓ Java代码函数分离
- ✓ 虚拟机指令保护（VMP）
- ✓ Java2CPP
- ✓ 防Java层调试
- ✓ 防native层调试
- ✓ 防调用

iOS SDK（framework)

- ✓ iOS源码混淆

SO文件

- ✓SO加固

安全加固——安全清场SDK

爱加密 www.ijiami.cn

Android 清场SDK：

- 框架攻击检测
- 注入攻击检测
- 调试攻击检测
- 劫持攻击检测
- 模拟器检测
- ROOT检测
- 应用多开检测
- 病毒、木马、恶意软件检测

iOS清场SDK：

- 越狱检测
- 重签名检测
- Cydia Substrate框架检测
- 逆向工具检测
- 代码注入框架检测
- 调试器检测
- 反调试器检测
- 发布渠道检测
- 代码段验证
- 网络代理检测
- airplay录屏和系统截屏录屏通知
- 后台开启模糊效果

安全加固——兼容性测试服务

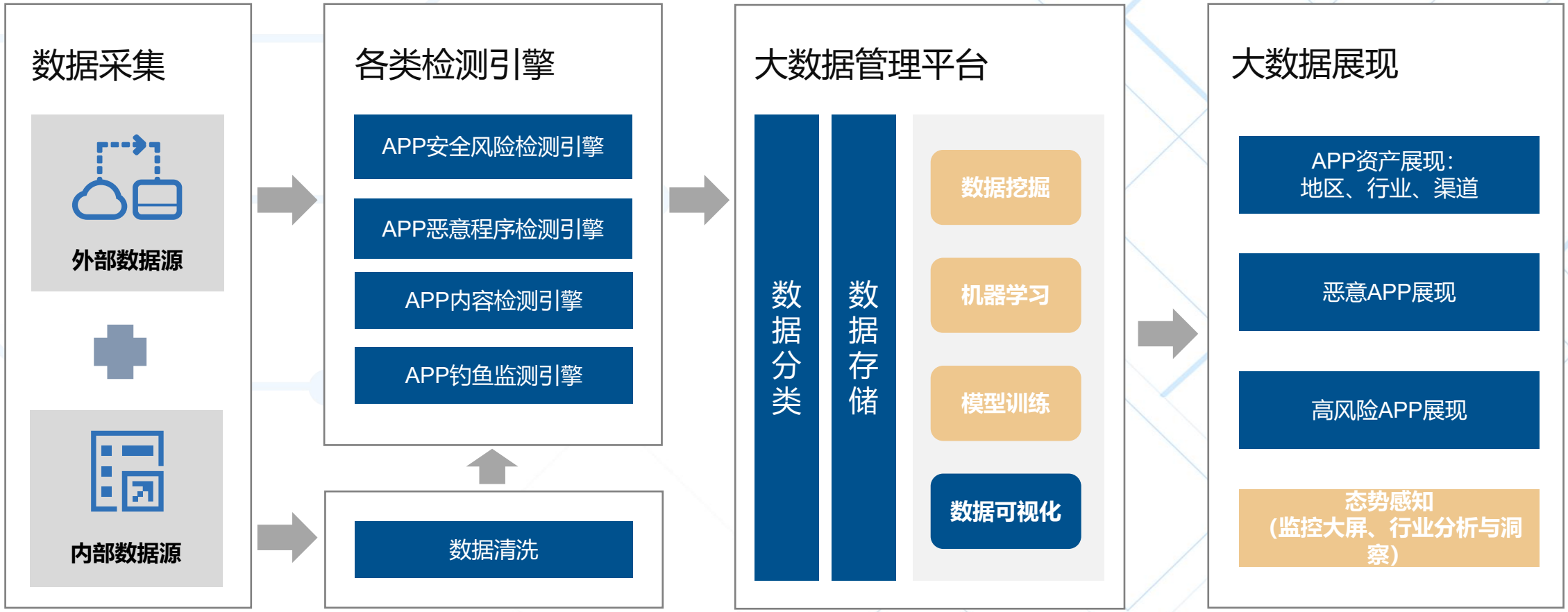
爱加密 www.ijiami.cn

爱加密加固后应用兼容性影响及性能指标	
CPU占用率增加量	小于5%
内存占用量增加量	小于5%
启动时间增加量	小于1秒
客户直观体验	无卡顿，无影响
包大小增加量	-5%——5%
加固后应用支持CPU架构	ARM，X86
加固后应用支持的标准安卓系统版本	Android2.2~Android10.0
加固后应用支持的深度定制系统	支持主流各大厂商深度定制系统

- 300款真机测试（标准服务）
- 3个工作日内
- 原包、加固包
- 适配性、兼容性
- 兼容性测试报告
- 最多1000款真机资源

安全维度——安全监测

爱加密 www.ijiami.cn



移动应用安全监管大数据平台

安全监测——内容监测

爱加密 www.ijiami.cn

色情

色情

低俗

性感

涉政

政治敏感人物

暴恐

国旗国徽

恐怖主义

枪支道具

血腥暴乱

检测依据：网安、网信办监管合规要求

- 十万级违规敏感词库，涵盖各类敏感信息
- 亿级实时更新图像样板库
- 深度学习图片识别技术
- 海量实时文本库

检测特点：

- 人工智能IA
- 智能语意分析能力
- 文字变体识别能力
- 检测对象类型包括：微信、qq、手机号、网址、公众号、百度搜索、微博、广告法等
- 适用场景包括：发帖、弹幕、评论、个人描述、私信、群聊、昵称等

安全监测——钓鱼监测

渠道监测系统是APP渠道信息管理平台，包括渠道数据监测、盗版APP识别与分析。开发者通过使用渠道监测服务可以方便的管理APP的推广渠道，掌握有关渠道信息；渠道监测平台还可以帮助开发者第一时间发现盗版APP，保护公司的合法权益。

渠道监测系统实现以下功能：

1) 对上传的APK文件进行渠道监测；
2) 对发现的盗版应用进行一键分析；
3) 对监测到的盗版应用进行预警；
4) 查看APP市场应用情况；
5) 建立应用数据样本库；
6) 支持创建新用户，并为用户指定监测渠道；

爬虫技术和渠道检测

通过应用名称遍历移动应用渠道市场，爬取渠道中存在的应用信息，获取诸如应用名称、版本、下载链接、下载量等应用基本信息。

盗版分析和下架

针对盗版APP提供定制化的人工分析服务

正版盗版精准对比分析：盗版分析项目涵盖APK所有路径文件，包括：需支持盗版分析项目涵盖APK所有路径文件及代码，包括：ACTIVITY，SERVICE，RECEIVER，PROVIDER，权限，源码，RES目录，META-DATA信息，SO库、AndroidManifest.xml等

B

管理维度

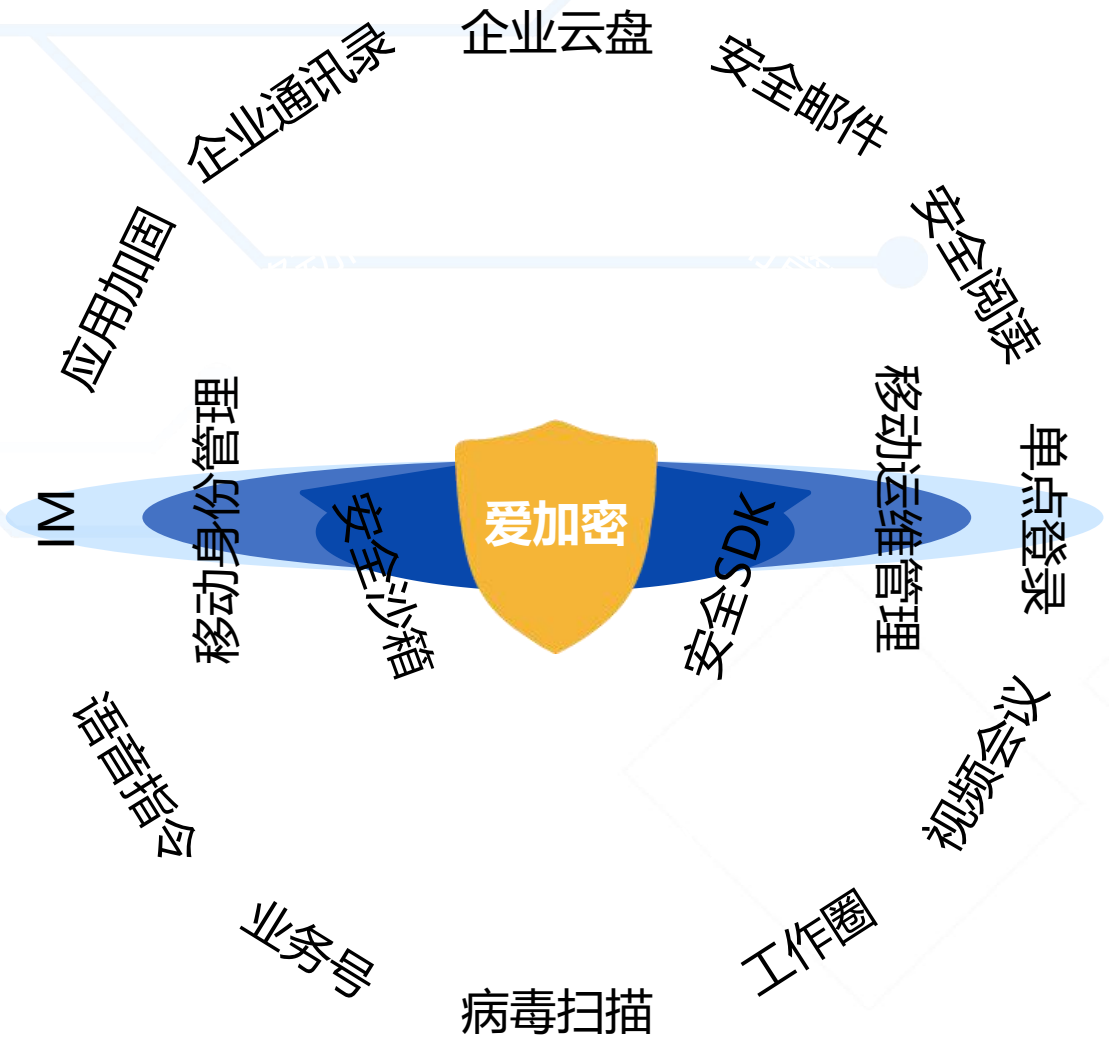
1、身份管理

2、应用管理

3、设备管理

4、运维管理

管理维度——移动安全管理平台架构模型



五大创新技术

- AppTunnel、安全沙箱、安全SDK、Android 虚拟空间、智能管理

六大核心功能

- 移动身份管理、移动设备管理、移动应用管理、移动内容管理、移动运维管理、移动安全服务

扩展应用模块

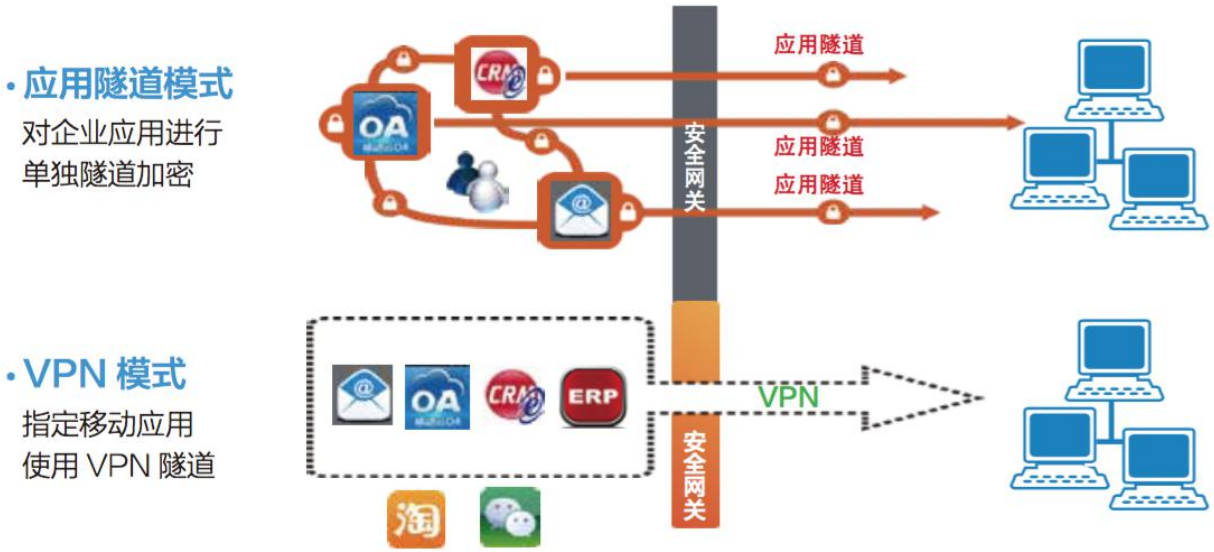
- 自研扩展应用
- 生态扩展应用

管理维度——创新技术

爱加密 www.ijiami.cn

AppTunnel 安全隧道

AppTunnel 安全隧道,支持标准加密或国密(可提供商密标准),高并发和极速转发的处理 能力,并且支持 TCP(http / https / socket)及 UDP 协议,支持各种动态端口应用,满足 企业各种移动应用的安全传输需求。



- 支持对用户、设备、应用三个维度实现独立的隧道开启、关闭管理;
- 使移动业务避免暴露在公网上,防止业务服务遭受外部攻击;
- 提供了对 HTTP 数据流量进行内容审计,可实现对 HTTP 业务的各种操作统计、分析。

管理维度——创新技术

Android 虚拟空间技术

爱加密在Android 系统中创建一个运行于系统之上的容器,为企业移动App 提供一个独立于本地 Android 系统的软件运行环境。不需要对企业的原有移动应用 APP 进行调整,直接进行发布,就能得到 EMM 系统的安全保护,包括数据安全存储、数据安全传输、移动数据防泄漏等，确保移动应用和数据的安全性,提升管理效率和用户体验。

管理维度——创新技术

安全沙箱

爱加密在终端上提供安全沙箱,在移动终端上,创建一个私有的文件系统,保证终端上存 储的数据安全,支持 AES256 加密算法(或国密算法),密钥分离存储,有效保证沙箱数据 的安全;沙箱性能极高,用户无感知,完全不影响应用体验;功能全面,可控制沙箱文件防 截屏、防分享、防拷贝、防另存,控制沙箱文件安全阅读(可定义水印),沙箱文件审计。

管理维度——创新技术

安全 SDK

安全能力植入

爱加密首创的 EMM SDK 交付模式，提供了全新的用户体验和个性化 EMM。移动门户开发商可使用 EMM SDK，迅速将其产品升级为具备全部 EMM 安全管理能力的超级 APP。

使用 EMM SDK，企业可以实现员工统一的超级入口，将安全、基础应用完全整合在一个 APP 中，便于企业推广 APP，也极大地改善了员工使用体验。

管理维度——创新技术

爱加密
www.ijiami.cn

智能管理

爱加密系统具有日志智能分析、机器学习、数据挖掘等智能管理能力。

学习并分析用户使用应用行为习惯,推荐企业移动应用,及发现异常访问;

日志智能统计分析,形成相应报表,提高运维人员工作效率;

根据服务器及网络等负载的情况,实现对移动应用的自动智能分批分发;

智能应用打包工具,可自动对 iOS 或 Android 应用进行二次打包。

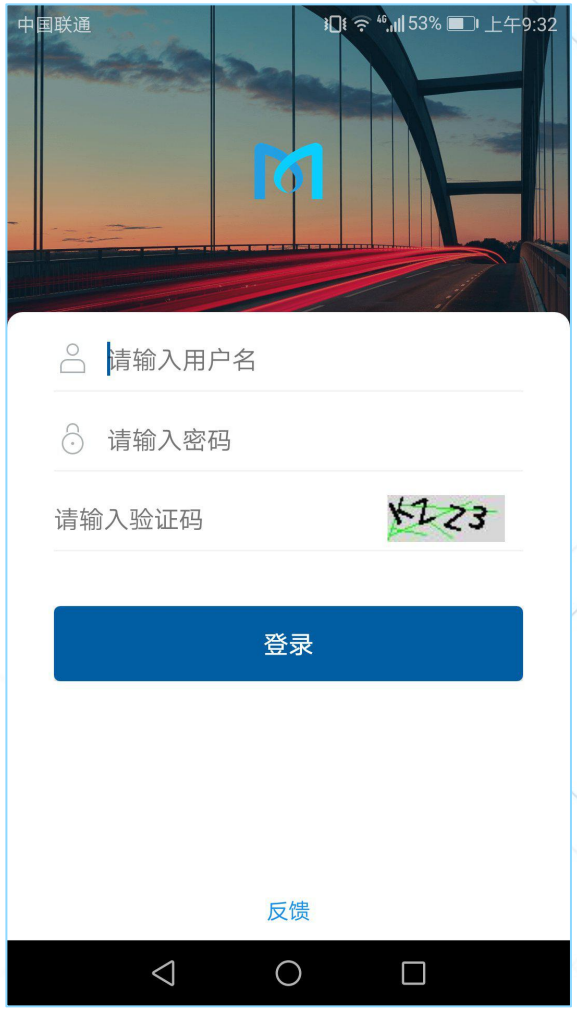
身份管理——用户认证

核准用户真实身份，禁止非法用户接入

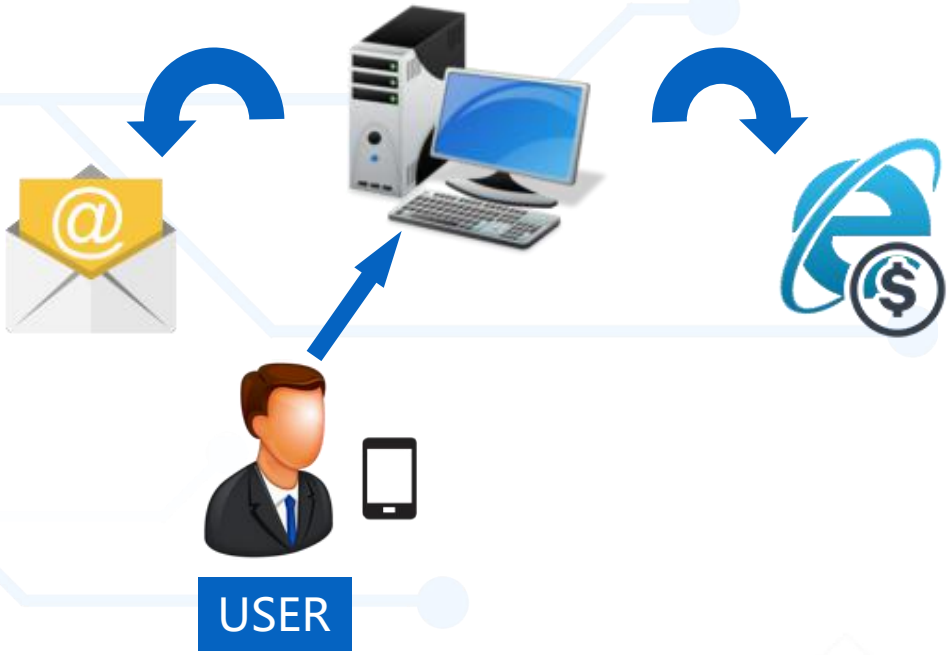
- 内置用户帐号管理功能、对接LDAP/AD、Radius等认证系统
- 用户名/密码，手势验证码、指纹登录、人脸识别登录等
- 内置动态口令（TOTP算法），支持邮件、短信网关对接
- 内建CA认证中心

身份管理 —— 登录认证

- 首次登录
  - 账号密码、验证码、动态口令等，身份强认证，同时完成手势密码设置、设备接入授权，设备绑定等
- 后续登录
  - 通过手势密码、数字密码等方式，
  - 实现账号登录



身份管理——单点登录（SSO）



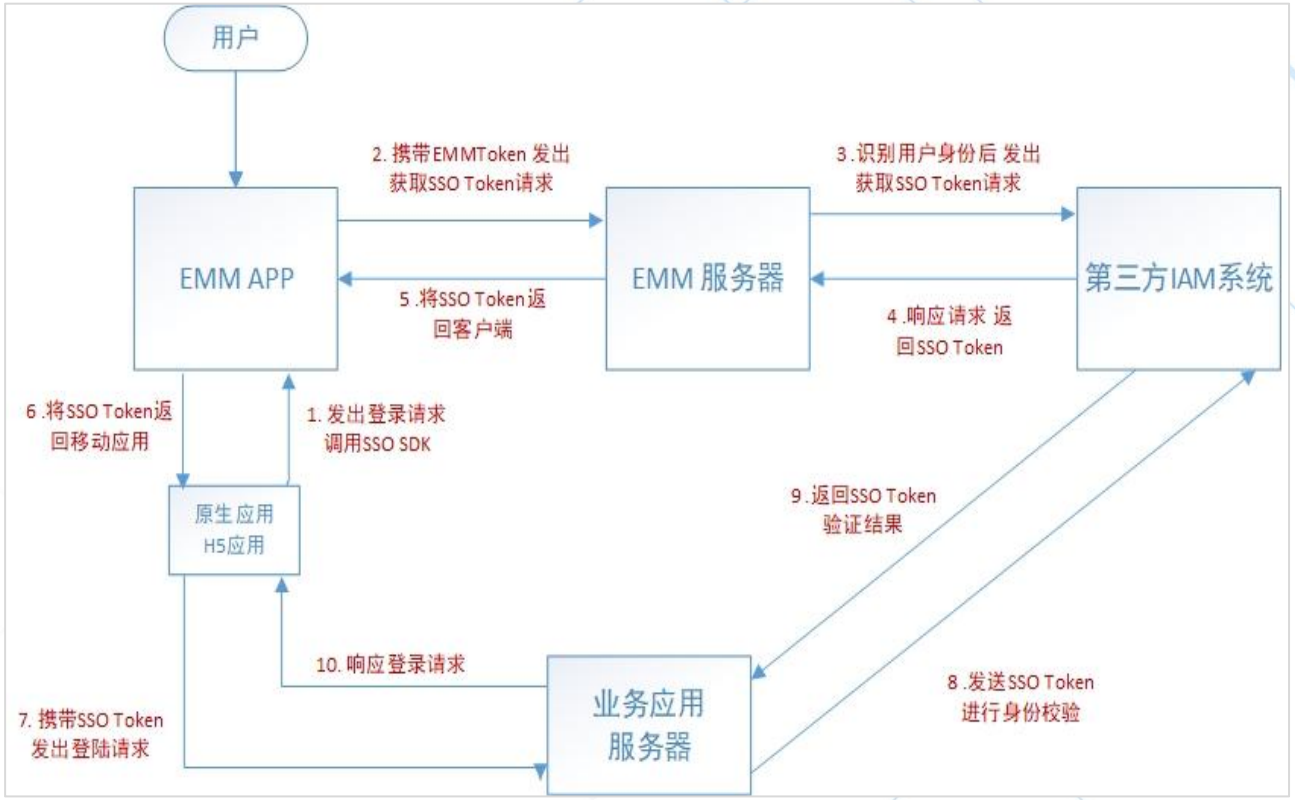
自有移动SSO单点登录方案

- 提供移动端SDK、后台.jar
- 支持HTML5、原生APP等

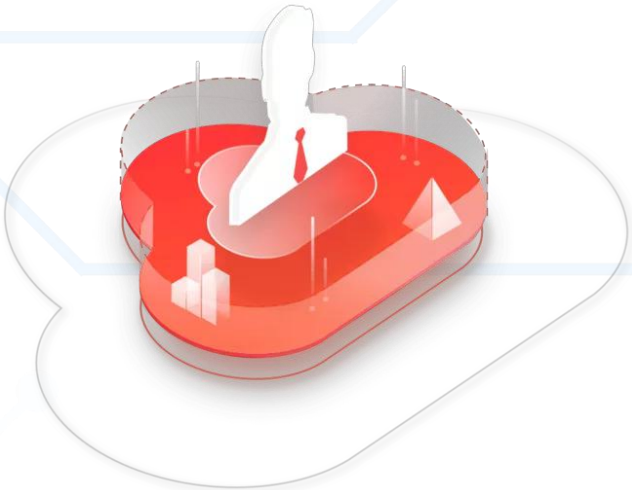
密码代填功能

- 对无法集成SSO应用，达到单点登录

单点登录流程



应用管理



- 实现对企业内部移动应用的统一发布上线
- EMM客户端下载，支持用户身份认证下载，只有授权的用户才能下载客户端，保证私有发布
- 应用智能分发，基于服务器及带宽负载动态调整发布上线进度
- 资源服务器支持独立部署，采用FAST文件系统，支持超大规模用户量应用分发

- Android系统原生应用，虚拟空间直接发布上线
- iOS系统原生应用，在线自动打包发布，防止企业证书外泄
- H5轻应用及PC WEB应用，直接发布上线

内容管理——移动数据防泄漏

- **MDM技术**
  - 终端应用防截屏（禁止截屏及截屏行为审计）
  - 移动应用页面水印覆盖
  - 远程移动数据擦除
- **沙箱技术**
  - 离线数据保护
  - 邮件内容安全存储
  - 办公文件安全阅读
  - 文档防复制（禁止内容复制/粘贴等）
- **数据分享管理**
  - 终端文档分享（微信、微博、QQ）等，提供权限控制、日志审计
- **基于策略的移动数据防泄漏**

设备管理——设备与用户绑定

用户与设备绑定，安全策略下发

EMM Client

用户首次登录：发送用户信息、密码等

认证通过

管理员

授信设备方可接入网络

创建手势密码、上传设备信息

设备审核通过，完成用户与设备绑定

系统安全策略下发：安全扫描/Root审核/应用黑名单/颁发证书文件

设备注销/丢失，员工离职

远程数据擦除/终端外设禁用

设备管理 —— 管控力度，按需定义

爱加密
www.ijiami.cn

MDM：EMM基础功能

爱加密协助企业IT部门，对访问企业内网的所有移动终端设备进行统一管理，根据不同场景配置相对应的安全管控策略，不管是BYOD还是企业专用配发设备都能有针对性地定义安全管控模式，使接入的移动终端设备符合企业安全访问标准。

设备管理 —— 企业专属设备管理

- 禁止用户私自安装/卸载应用
- 虚拟工作桌面模式
- 将某一应用限定在前台，无法退出
- 禁止用户设置/修改锁屏密码

运维管理

- **系统实时监控**
  - 统计分析平台系统资源实时占用情况
- **系统进程监控**
  - 实时监控平台系统关键进程运行情况
- **移动应用流量监控**
  - 实时监控移动应用流量带宽使用情况
- **安全事件运维管理**
  - 管理员预定义安全事件及处理流程，系统自动对发生的安全事件，进行跟踪处理

运维管理——安全审计

爱加密 www.ijiami.cn

- 企业应用访问审计
- 截屏行为审计
- 沙箱文件审计
- 文件外发分享审计
- 客户端运行日志
- 客户端隧道代理转发日志
- 网关数据转发日志
- 后端服务日志

爱加密
www.ijiami.cn

谢谢欣赏

洞悉移动风险 智领安全未来

电话：010-82825622

网址：www.ijiami.cn

地址：北京市海淀区中关村软件园10号楼207-2（国永融通）