

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

目录 >>>

CONTENTS

- ▣ 01 公司介绍
- ▣ 02 背景介绍
- ▣ 03 解决方案

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+



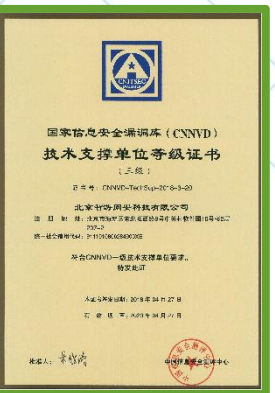
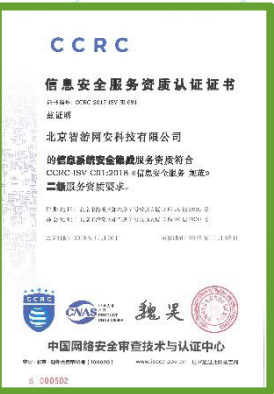
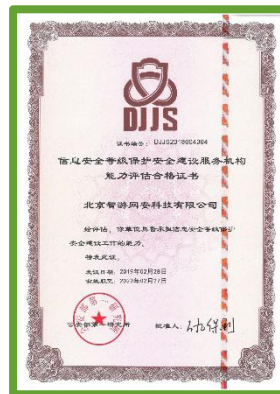
智能终端设备
10亿+



公司介绍——企业资质



- 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信息安全管理体系统认证证书
- 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+)



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

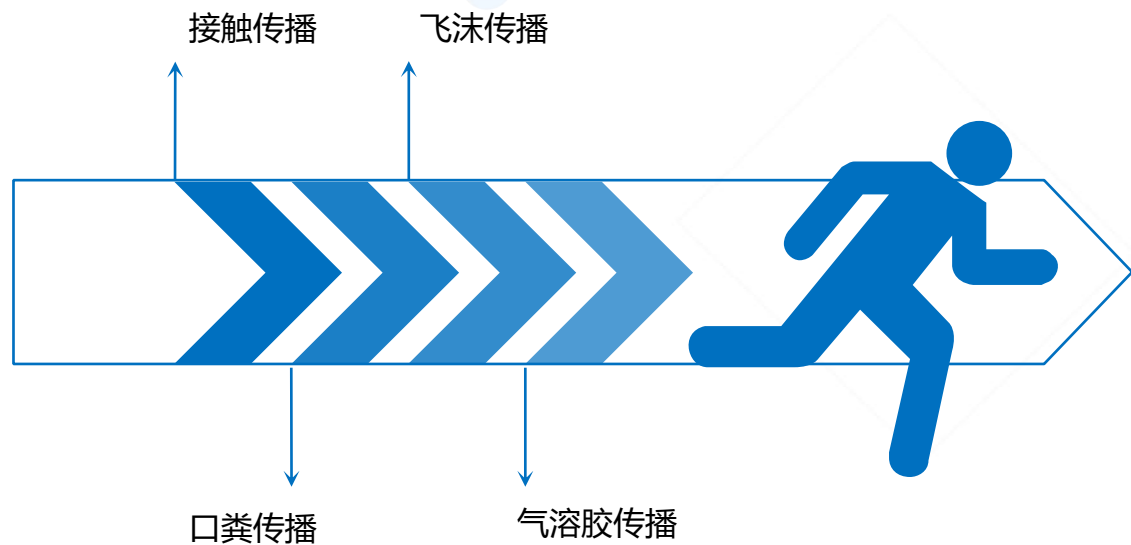


02 背景介绍

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↓
跟谁学 GSX	44.98	18.81%
有道 DAO	25.40	14.31%
无忧英语(51) COE	22.52	10.39%
好未来 TAL	59.40	2.48%
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



03

解决方案介绍



远程移动办公安全解决方案



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

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



动态运行时漏洞检测

- ☐ C层代码动态调试漏洞
- ☒ 输入监听漏洞
- ☐ 动态代码注入攻击漏洞
- ☐ App篡改/二次打包攻击漏洞

资源文件安全规范检测

- ☐ H5文件明文存储检测
- ☐ 图片冗余数据检测
- ☒ 证书文件明文存储检测
- ☒ 资源文件_篡改分析检测

系统常用类配置安全规范检测

- ☒ Intent检测
- ☒ 动态加载DEX文件检测

程序机密性规范检测

- ☒ 代码混淆检测
- ☒ DEX保护检测
- ☐ DEX加花保护
- ☐ SO保护检测
- ☒ 应用完整性_功能实现检测
- ☐ 应用完整性_代码安全检测
- ☐ 程序安全_功能实现检测

四大组件配置安全规范检测

- ☒ Activity权限攻击检测
- ☐ Activity劫持检测
- ☒ Activity数据残留检测
- ☒ Activity敏感数据泄露检测
- ☒ Activity身份验证
- ☒ Broadcast Receiver检测
- ☒ Service权限攻击检测

移动应用基本信息检测

- ☒ 应用信息检测
- ☒ 应用签名信息检测
- ☒ 应用行为信息检测
- ☒ 应用权限信息检测
- ☒ 应用加固识别

移动应用恶意行为检测

- ☐ 病毒检测
- ☒ 敏感行为检测
- ☒ 敏感函数检测
- ☒ 敏感词汇检测

四大组件配置安全规范检测

- ☐ 模拟器检测
- ☒ Java调试检测
- ☒ 第三方SDK检测
- ☒ 资源文件中包含apk
- ☐ 运行其它可执行程序检测

应用级漏洞检测

- ☒ WebView远程代码执行漏洞
- ☐ APK静态反编译漏洞
- ☒ 下载任意APK漏洞
- ☐ 数据库注入漏洞
- ☒ SecureRandom猜解漏洞

数据安全规范检测

- ☒ 调试信息检测
- ☒ 测试数据移除检测
- ☒ 内网信息残留检测
- ☒ 异常处理检测
- ☒ SD CARD数据储存检测
- ☐ 数据传输安全检测
- ☐ Content Provider数据储存检测

代码安全规范检测

- ☒ 硬编码检测
- ☒ SSL证书使用规范检测
- ☒ WebView组件忽略SSL证书验证错误检测



检测项

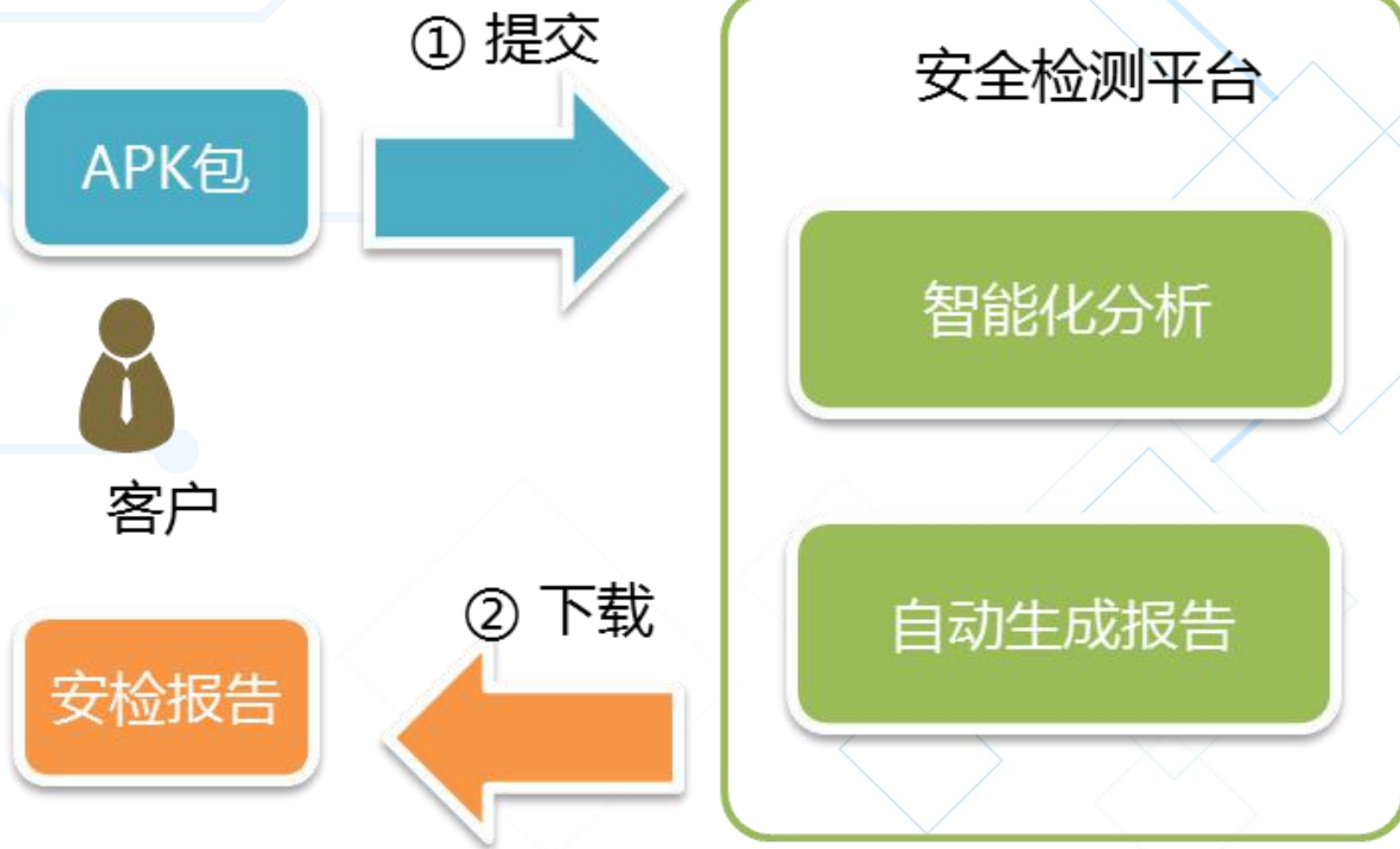
Android: 75项

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

爱加密移动应用安全检测系统

当前位置: 资产中心

全部应用 (70) Android应用 (70) iOS应用 (0)

请输入应用名称

上传多个文件

上传单个文件

Android

WeChat6.6.7

检测次数: 3
最后一次检测分数: 34分 (无)
上传者: xiangpeng

Android

全民点游2.1.1

检测次数: 3
最后一次检测分数: 39分 (无)
上传者: zhangkui

Android

苏宁金融6.0.0

检测次数: 1
最后一次检测分数: 34分 (无)
上传者: sup_ijiami

Android

iCapture1.0

检测次数: 28
最后一次检测分数: 84分 (无)
上传者: xiangpeng

Android

CSD

广场舞中国2.4.4

检测次数: 5
最后一次检测分数: 43分 (无)
上传者: xiangpeng

Android

夏老师1.2.0

检测次数: 1
最后一次检测分数: 34分 (无)
上传者: xiangpeng

爱加密移动应用安全检测系统

上传应用

文件上传 URL上传

选择应用

请上传小于1GB的apk包文件

第一步, 点击选择应用

第二步, 点击保存

取消 保存



安全评估——自动安全检测



爱加密移动应用安全检测系统

您好, 超级管理员

资产中心

任务管理

检测配置

检测项

检测模板

敏感词库

敏感权限库

控制中心

系统管理

当前位置: 检测模板

检测模板配置: 自定义配置不同的检测模板

序号	模板名称	检测项数量	适用系统
1	111	8	android
2	默认8	8	android
3	www	8	android
4	mm	7	android
5	默认2	8	android
6	默认1	7	android
7	默认	8	android
8	测试2	12	android
9	测试1	9	android
10	默认8项	7	android

爱加密移动应用安全检测系统

您好, 超级管理员

资产中心

任务管理

检测配置

检测项

检测模板

敏感词库

敏感权限库

控制中心

系统管理

当前位置: 检测模板

新建检测模板

检测项目:

☐	序号	检测项名称	检测分类 (全部)
☒	1	基本信息检测	基本信息
☒	2	应用权限检测	基本信息
☒	3	应用行为检测	基本信息
☒	4	第三方SDK检测	基本信息
☒	5	恶意程序检测	基本信息
☒	6	越权行为检测	基本信息
☒	7	权限滥用风险	基本信息
☐	8	敏感词库检测	内容
☐	9	启动隐藏服务风险	源文件风险
☐	10	动态加载外部代码风险	安全策略风险

共 74 条 10 条/页

1 2 3 4 5 6 ... 8 前往 1 页

取消 确定

检测项配置: 其中高中低危风险监测项一共有75项



安全评估——自动安全检测

安全检测评估报告

XXXX


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

爱加密版权所有 ©2013-2016, 侵权必究

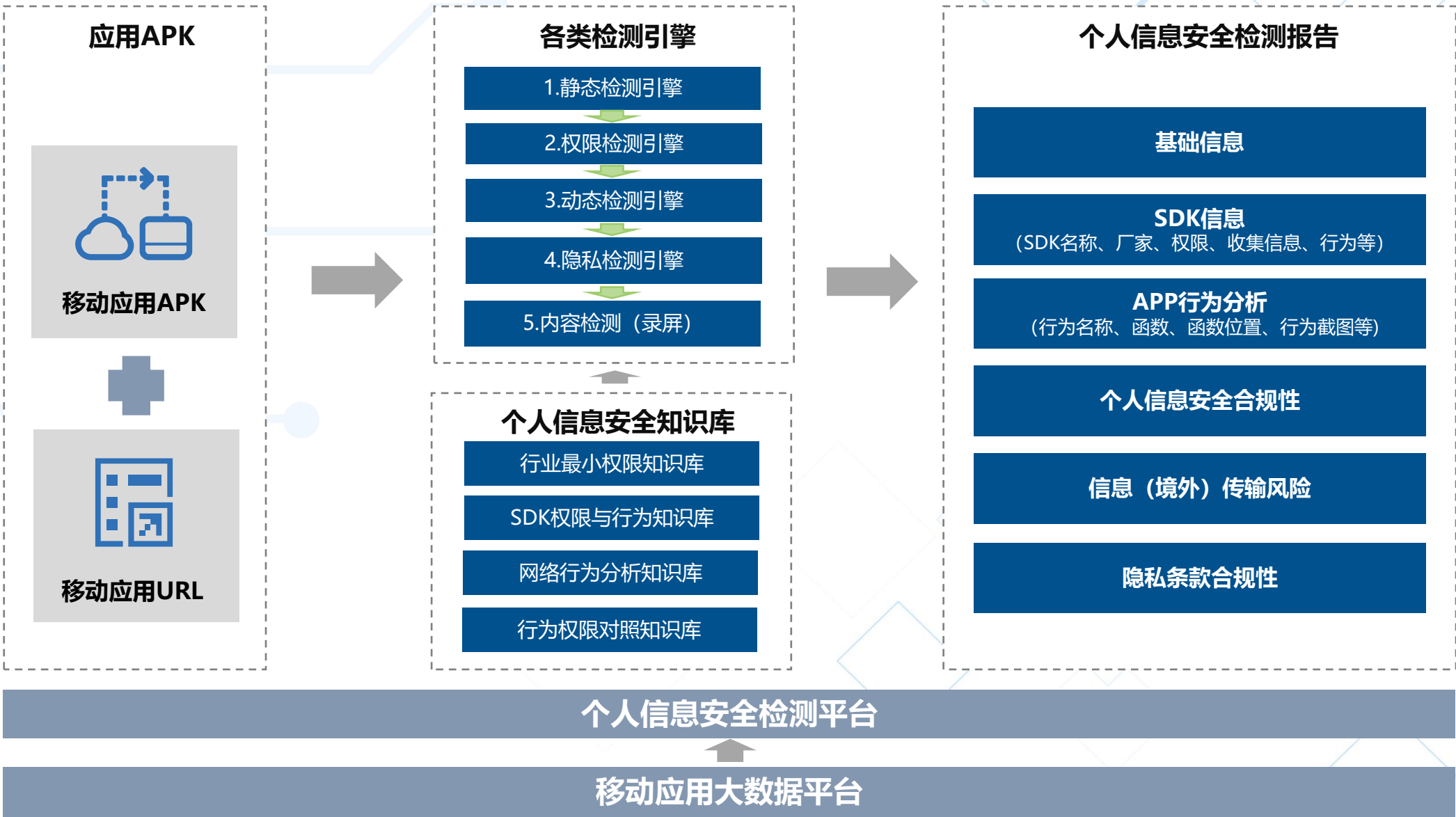
7	敏感行为检测	低危
8	敏感函数检测	安全
9	敏感词汇检测	低危
10	动态加载 DEX 行为检测	低危
11	代码混淆检测	安全
12	DEX 保护检测	高危
13	DEX 加花保护检测	中危
14	SO 保护检测	安全
15	应用完整性检测	安全
16	程序签名保护检测	安全
17	动态调试攻击检测	安全

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 Lcom/transfar/tradedriver/base/BaseActivity;-><init>()V return-void {p0};



安全评估——个人信息合规评估



安全维度——个人信息合规评估

上传移动应用

爱加密移动应用个人信息安全检测系统

< > | 资产中心 >

Android应用 (1001) iOS应用 (1001)

请输入应用名称或应用包名搜索

☐	序号	LOGO	应用名称	版本号	检测次数	检测模板	最后一次检测分数	最后一次检测时间	上传者	上传时间	操作
☐	1		支付宝	v8.6.9.104	3	默认模板	60	2018-10-23 17:37:00	张三	2018-10-23 17:37:00	查看隐私权限 开始检测 删除
☐	2		飞猪						管理员	2018-10-23 17:37:00	查看隐私权限 开始检测 删除
☐	3		建程网						系统	2018-10-23 17:37:00	查看隐私权限 开始检测 删除
☐	4		建程网						admin	2018-10-23 17:37:00	查看隐私权限 开始检测 删除
☐	5		建程网						admin	2018-10-23 17:38:00	查看隐私权限 开始检测 删除

共4条 10条/页 < 1 2 100 > 前往第 1 页

添加资产

资产类型 Android

上传方式 ☒ 本地上传 ☐ url上传

将文件拖到此处，或 [点击上传](#)

请上传小于1GB的apk文件

[保存](#) [取消](#)



安全评估——个人信息合规评估



检测报告



选择报告
模板

选择报告输出的文件
格式



安全评估——渗透测试

● 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



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

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

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

数据防泄漏

内存数据

日志数据

本地数据

SDK

数据传输

页面数据保护

SDK

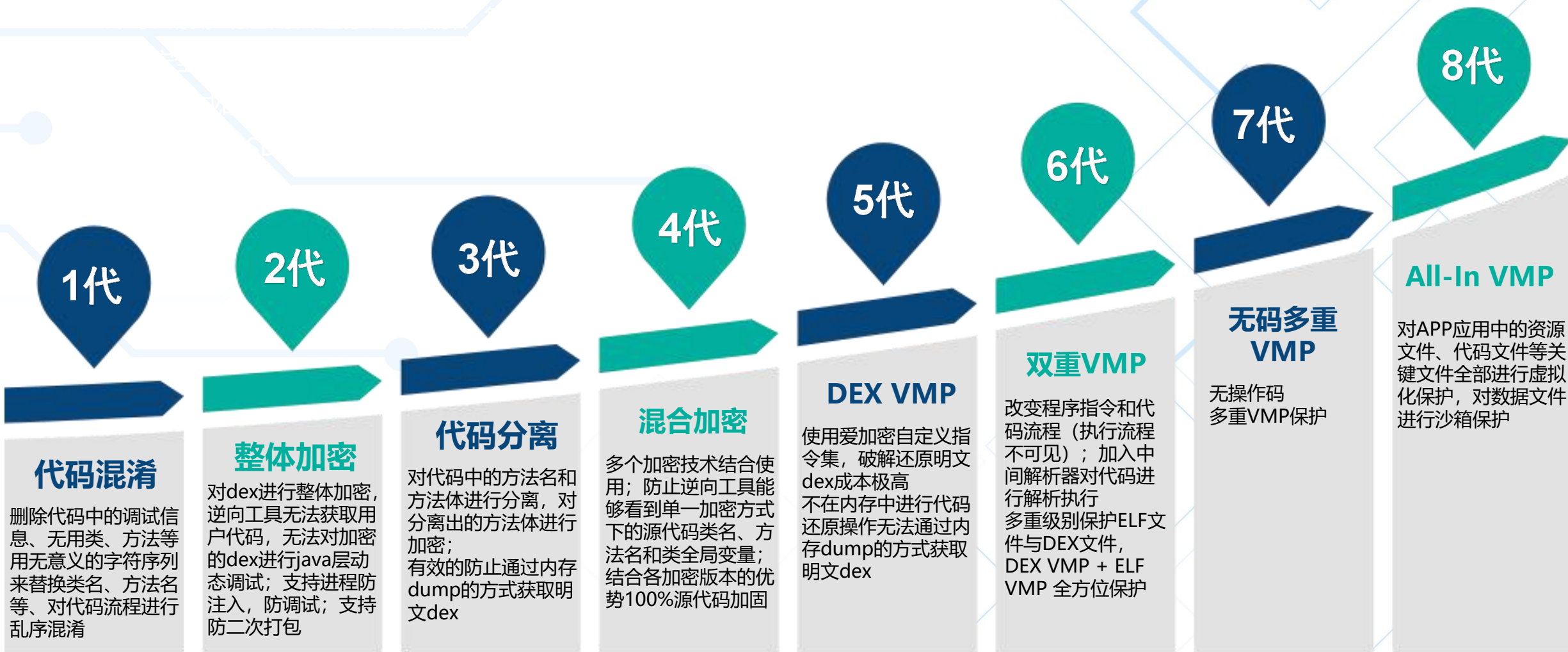
应用防截屏

应用防劫持

安全键盘

数据层面

安全加固——Android加固发展路线



安全加固——iOS应用加固

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

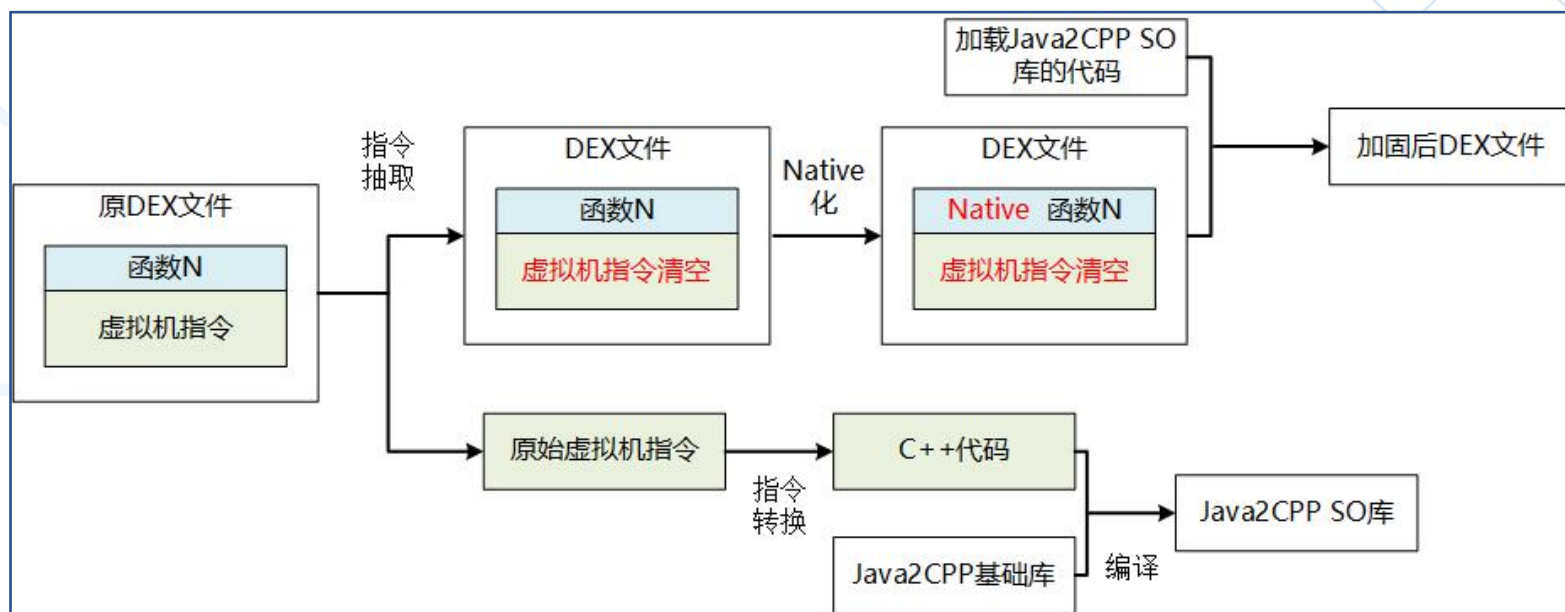
- ✓ 字符串加密
- ✓ 等效指令替换
- ✓ 基本块分裂
- ✓ 基本块调度
- ✓ 虚假控制流
- ✓ 控制流扁平化
- ✓ 控制流间接化

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)



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

□ 键盘防截屏

□ 键盘防劫持

□ 输入时，输入框无短暂明文显示



安全加固——安全键盘SDK (H5)



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



- 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

No.	Time	Source	Destination	Protocol	Length	Info
22	7.90676600	192.168.137.80	122.114.40.32	TCP	74	50794->9001 [SYN] Seq=0 win=14600 Len=0 MSS=1460
25	8.03205200	122.114.40.32	192.168.137.80	TCP	74	9001->50794 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0
26	8.14810700	192.168.137.80	122.114.40.32	TCP	66	50794->9001 [ACK] Seq=1 Ack=1 win=14656 Len=0
27	8.15133900	192.168.137.80	122.114.40.32	SSLV3	198	Client Hello
28	8.17461700	122.114.40.32	192.168.137.80	TCP	66	9001->50794 [ACK] Seq=1 Ack=133 win=30080 Len=0
29	8.17816300	122.114.40.32	192.168.137.80	SSLV3	894	Server Hello, Certificate, Server Hello Done
30	8.19933700	192.168.137.80	122.114.40.32	TCP	66	50794->9001 [ACK] Seq=133 Ack=829 win=17536 Len=0
31	8.20333900	192.168.137.80	122.114.40.32	SSLV3	278	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
32	8.22720800	122.114.40.32	192.168.137.80	SSLV3	141	Change Cipher Spec, Encrypted Handshake Message
33	8.27066300	192.168.137.80	122.114.40.32	SSLV3	236	Application Data, Application Data
34	8.29291400	122.114.40.32	192.168.137.80	SSLV3	236	Application Data, Application Data
35	8.32650200	192.168.137.80	122.114.40.32	TCP	66	50794->9001 [FIN, ACK] Seq=515 Ack=1074 win=19200
36	8.34989600	122.114.40.32	192.168.137.80	TCP	66	9001->50794 [FIN, ACK] Seq=1074 Ack=516 win=32768
37	8.35617800	192.168.137.80	122.114.40.32	TCP	66	50794->9001 [ACK] Seq=516 Ack=1075 win=19200

Filter: ip.addr == 122.114.40.32

Expression... Clear Apply Save

Frame 33: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface 0

Ethernet II, Src: Samsung_a7:e0:a0 (50:cc:f8:a7:e0:a0), Dst: Shenzhen_e8:80:3c (bc:96:80:e8:80:3c)

Internet Protocol Version 4, Src: 192.168.137.80 (192.168.137.80), Dst: 122.114.40.32 (122.114.40.32)

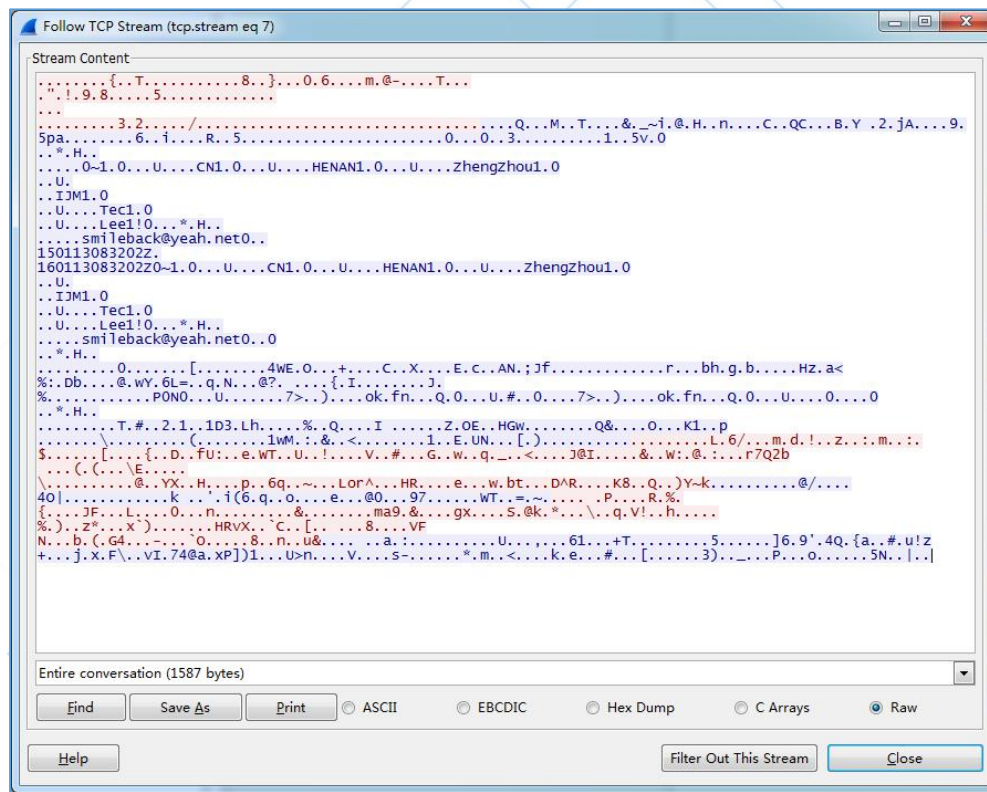
Transmission Control Protocol, Src Port: 50794 (50794), Dst Port: 9001 (9001), Seq: 345, Ack: 904, Len: 170

Secure Sockets Layer

- SSLV3 Record Layer: Application Data Protocol: Application Data
 - Content Type: Application Data (23)
 - Version: SSL 3.0 (0x0300)
 - Length: 32

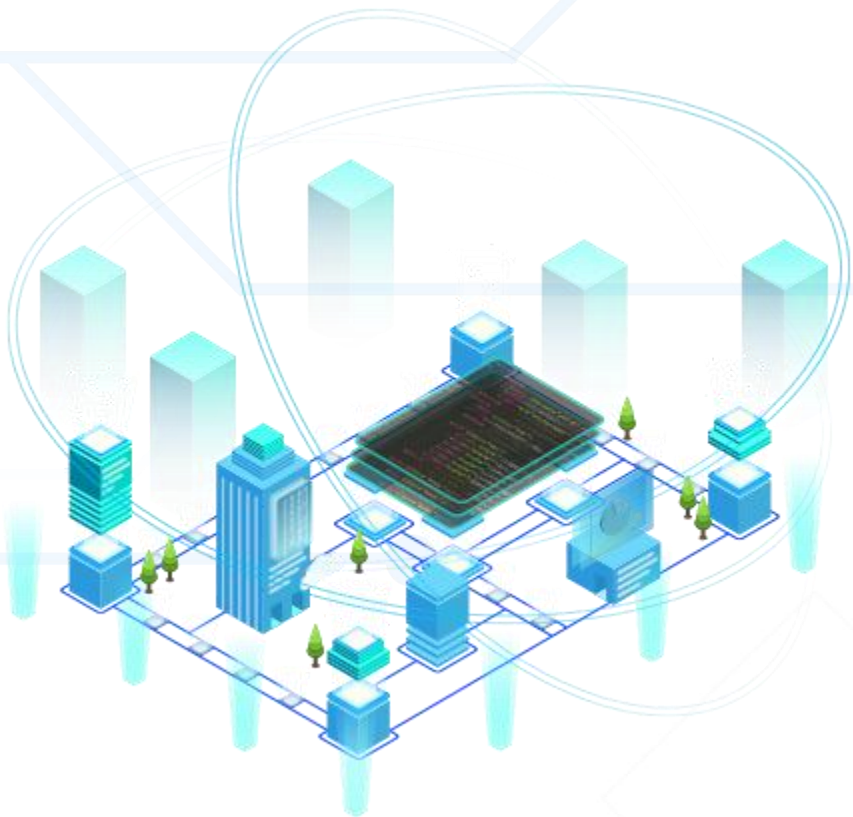
0000	bc 96 80 e8 80 3c 50 cc f8 a7 e0 a0 08 00 45 00	<P.....E.
0010	00 de f1 18 40 00 40 06 5c 76 c0 a8 89 50 7a 72	@.@. \v...Pzr
0020	28 20 c6 6a 23 29 b8 c0 21 95 6e 7b cc ab 80 18	(.j#)...!n{....
0030	01 12 8e 7a 00 00 01 01 08 0a 00 03 d1 79 0e 87	...Z.....y...
0040	2a c4 17 03 00 00 20 9a 50 95 97 99 a0 52 f8 25	*.....P.....R.%
0050	8e 0d 7b 15 8a c2 c0 4a 46 da ac e6 4c 98 1a f6	...{.....J F...L...
0060	f1 30 f8 d4 c2 6e 09 17 03 00 00 80 91 f9 17 26	..O...n.....&
0070	f9 cd 12 0b f3 96 88 19 6d 61 39 93 26 fe c2 c5	ma9.&...
0080	f5 67 78 83 1a e1 fe 53 af 40 6b de 2a 9e 8c 90	..gx...S.@k.*...
0090	5c 08 ad 71 97 56 21 bd 88 68 b0 17 b6 9d 1b 25	..Q.v!..h...%
00a0	1d 29 93 19 7a 2a 8d fc 82 78 60 29 fb 12 d8 db	..).z*...x')....
00b0	de bf fb 48 52 76 58 e5 da 60 43 af 18 5b 7f f9	...HRVX..`C.[...
00c0	20 9a e7 0c 38 c3 9d f9 83 56 46 0d 4e 06 08 dc	...8...VF.N...
00d0	62 19 28 e7 47 34 cc ff 16 2d ad b1 83 60 4f c2	b.(G4...-...O.
00e0	f7 d2 ee a9 38 fd b7 6e 9f f6 75 26	8..n..u&

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



JS控制流
扁平化

JS字符串
加密

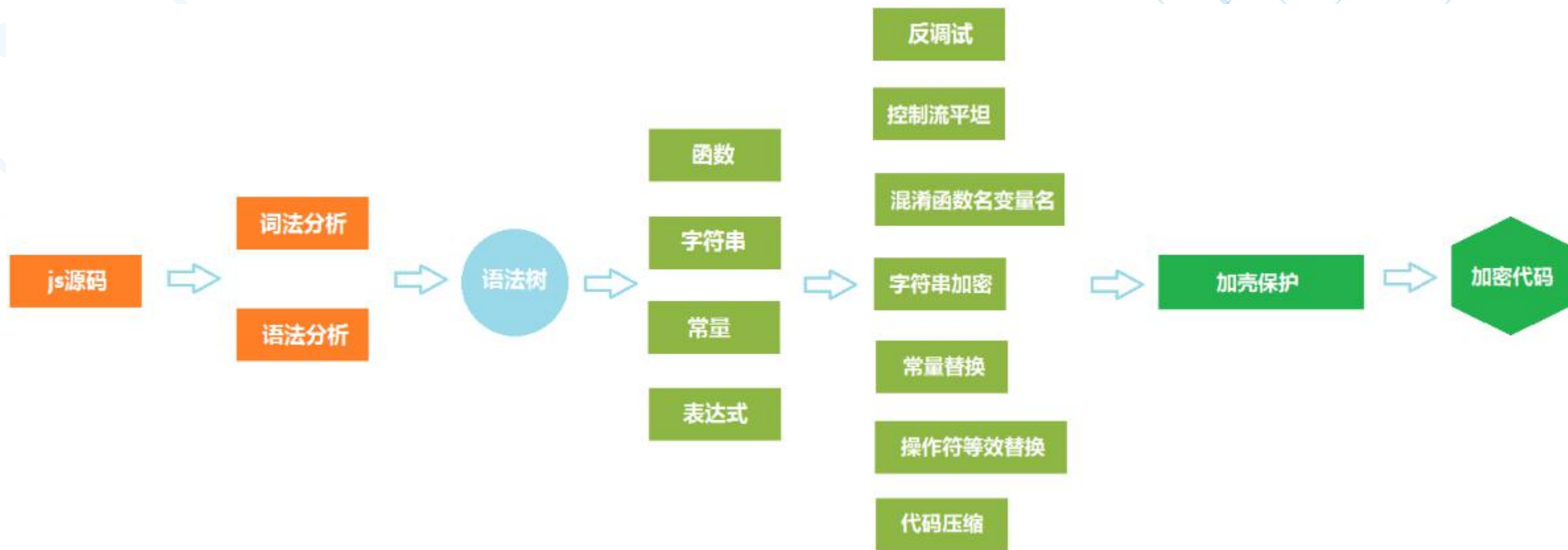
JS数字
加密

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

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



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



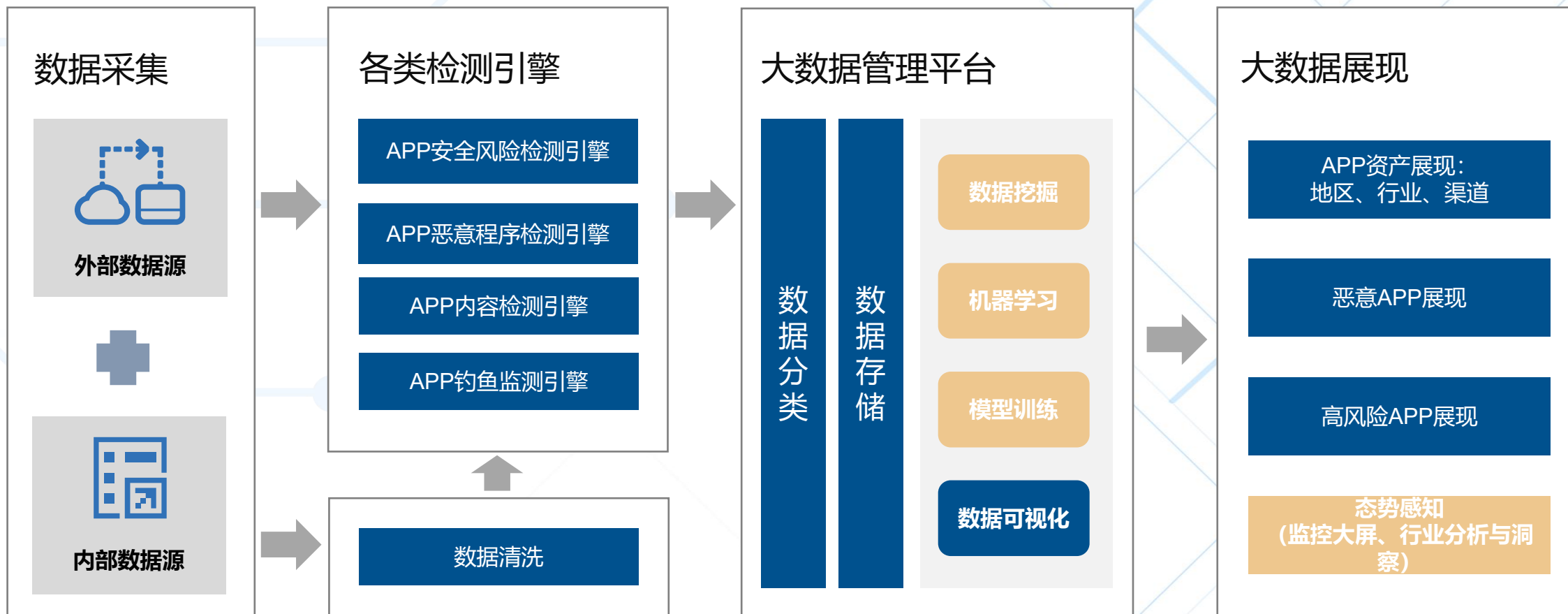
爱加密加固后应用兼容性影响及性能指标

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



移动应用安全监管大数据平台

安全监测——内容监测

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



精细化的场景分类

露胸、露阴、性爱场景、生殖器、
枪支、自焚场景、标志等.....

识别结果

色情



暴恐



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

渠道
监测

盗版
分析

盗版
下架

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

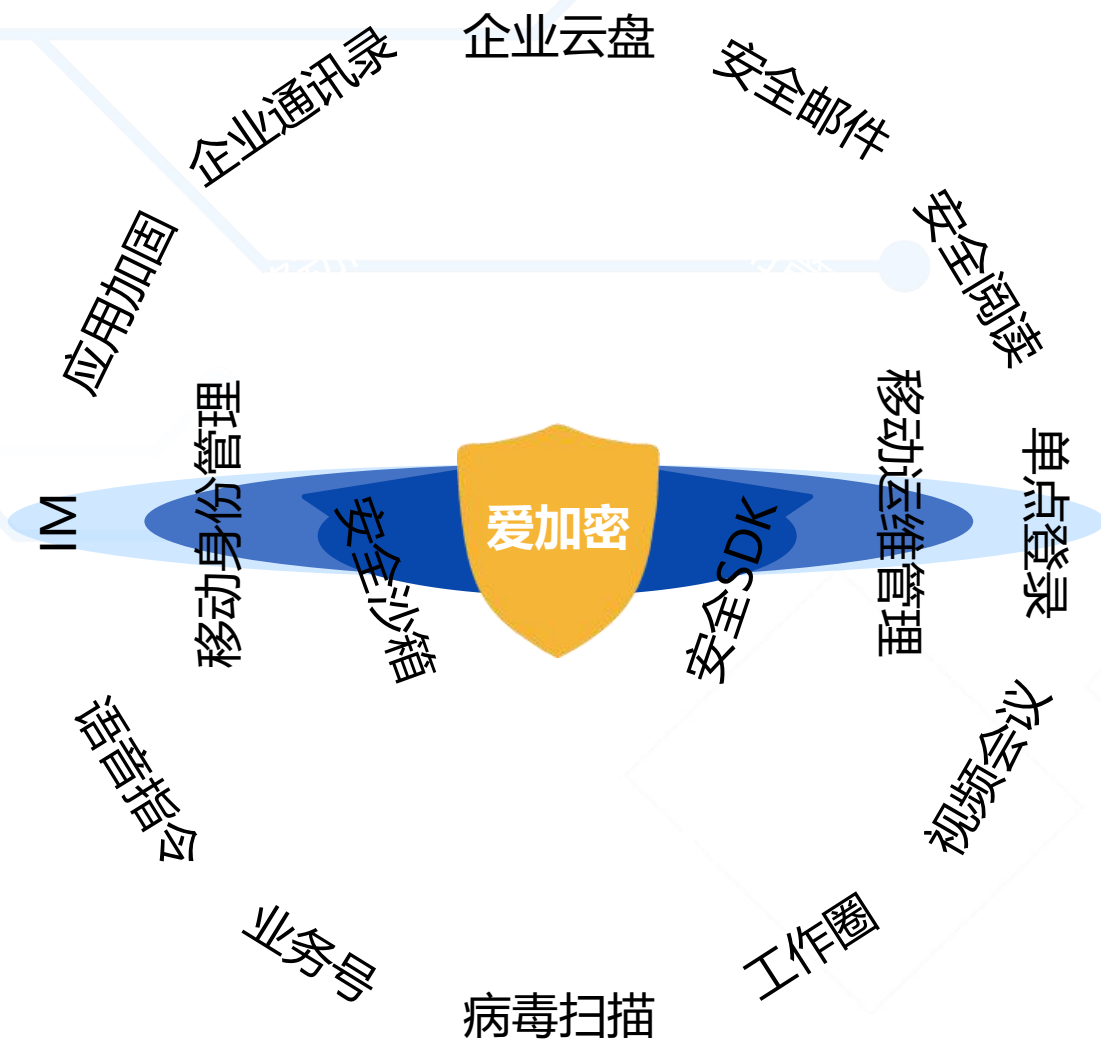
针对盗版APP提供定制化的人工分析服务
正版盗版精准对比分析：盗版分析项目涵盖APK所有路径文件，包括：需支持盗版分析项目涵盖APK所有路径文件及代码，包括：ACTIVITY，SERVICE，RECEIVER，PROVIDER，权限，源码，RES目录，META-DATA信息，SO库、AndroidManifest.xml等

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

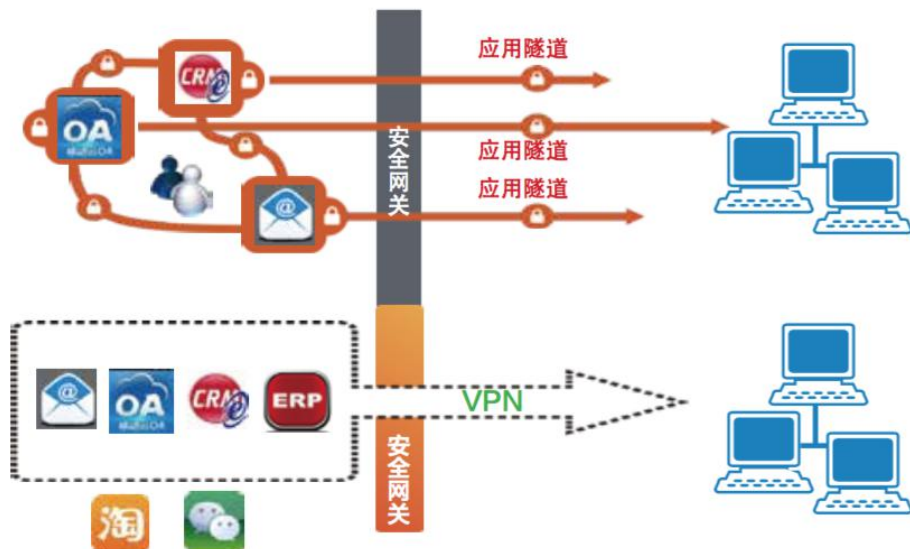
- 自研扩展应用
- 生态扩展应用

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。

• 应用隧道模式

对企业应用进行单独隧道加密



• VPN 模式

指定移动应用使用 VPN 隧道

- 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。

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

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。



身份管理——用户认证



核准用户真实身份，禁止非法用户接入

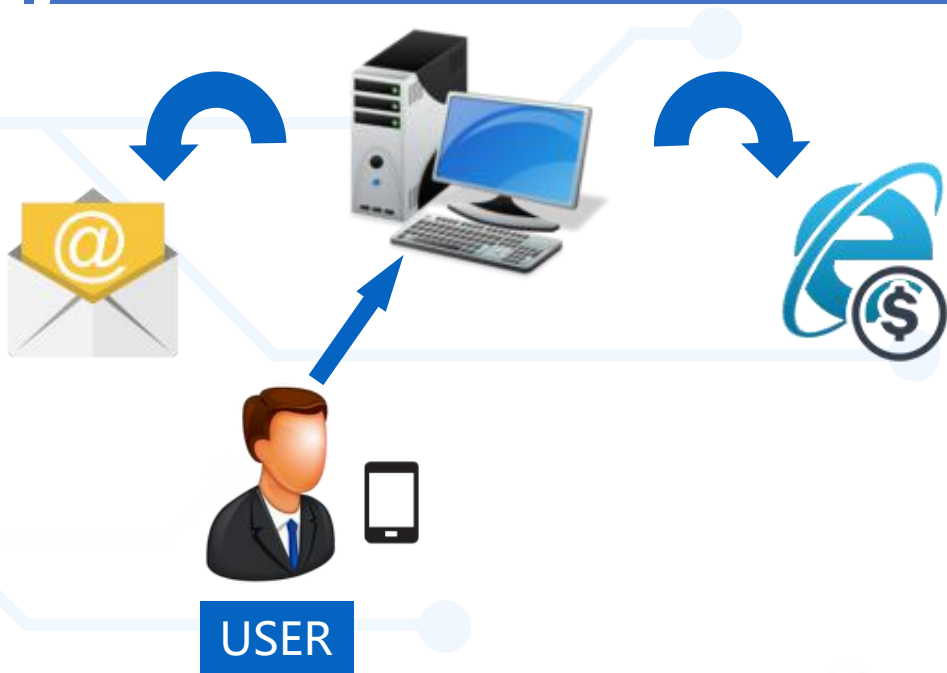
- 内置用户帐号管理功能、对接LDAP/AD、Radius等认证系统
- 用户名/密码，手势验证码、指纹登录、人脸识别登录等
- 内置动态口令（TOTP算法），支持邮件、短信网关对接
- 内建CA认证中心

身份管理 —— 登录认证

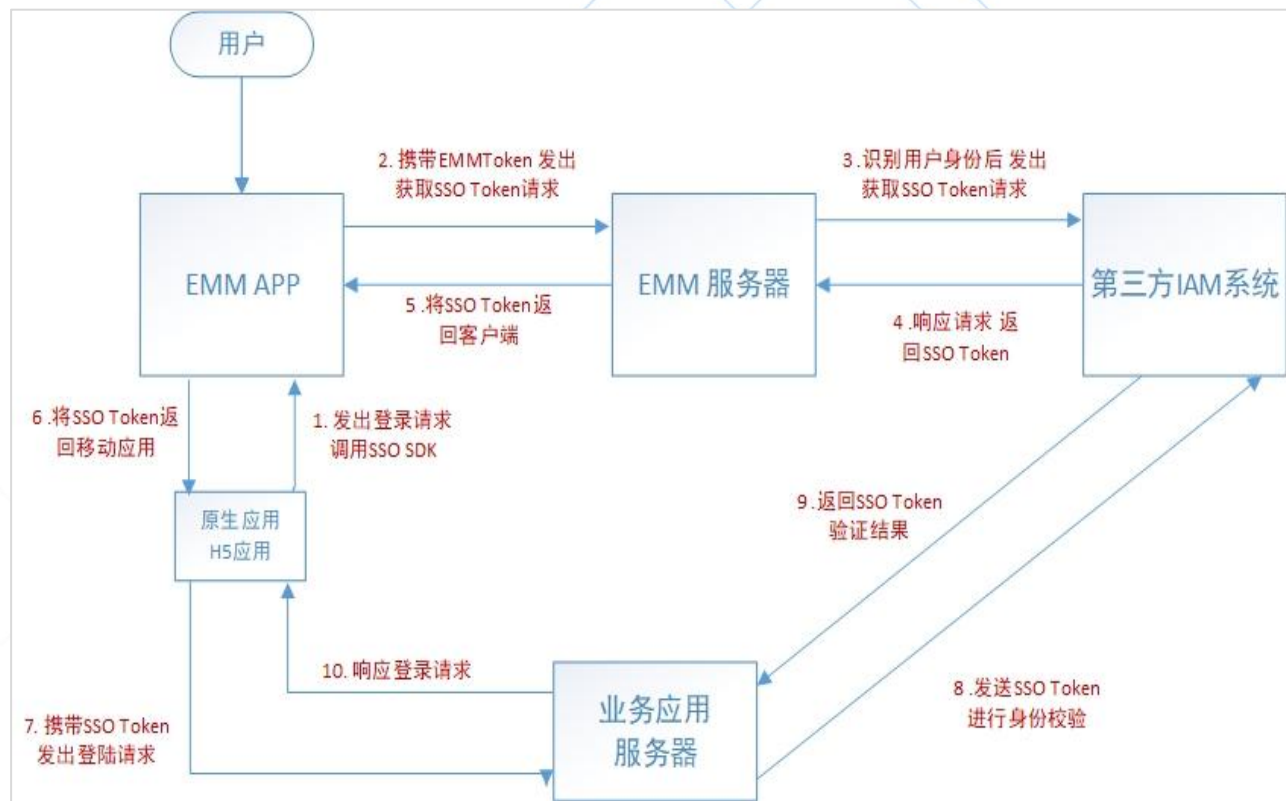
- 首次登录
 - 账号密码、验证码、动态口令等，身份强认证，同时完成手势密码设置、设备接入授权，设备绑定等
- 后续登录
 - 通过手势密码、数字密码等方式，
 - 实现账号登录



身份管理——单点登录 (SSO)

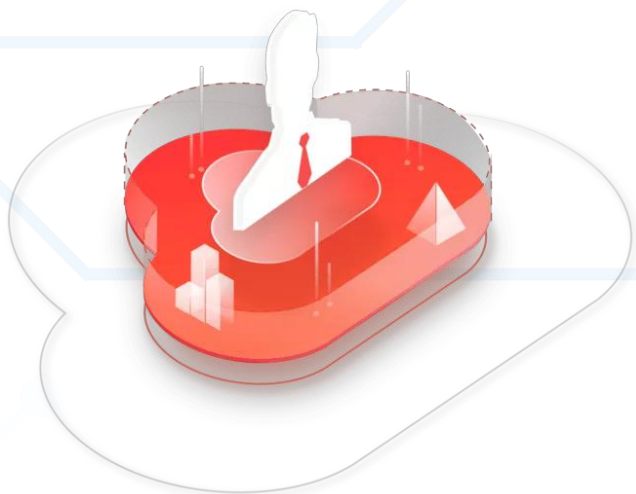


单点登录流程



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



- 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

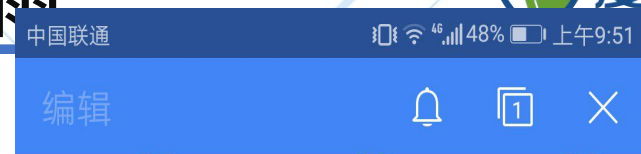
- **沙箱技术**

- 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**



民进中央：劳务所得税 800 元起征点已 36 年 建议提高

澎湃新闻宋江云

分享

45 评论

劳务所得税自 1980 年实施 800 元的起征点以来，已经有长达 36 年未进行调整。2017 年全国两会开幕在即，提高劳务所得税起征点呼声再起。

3 月 4 日，澎湃新闻(www.thepaper.cn)从民进中央获悉，民进中央拟在全

文件

查看



另存为



输出为pdf



分享



打印



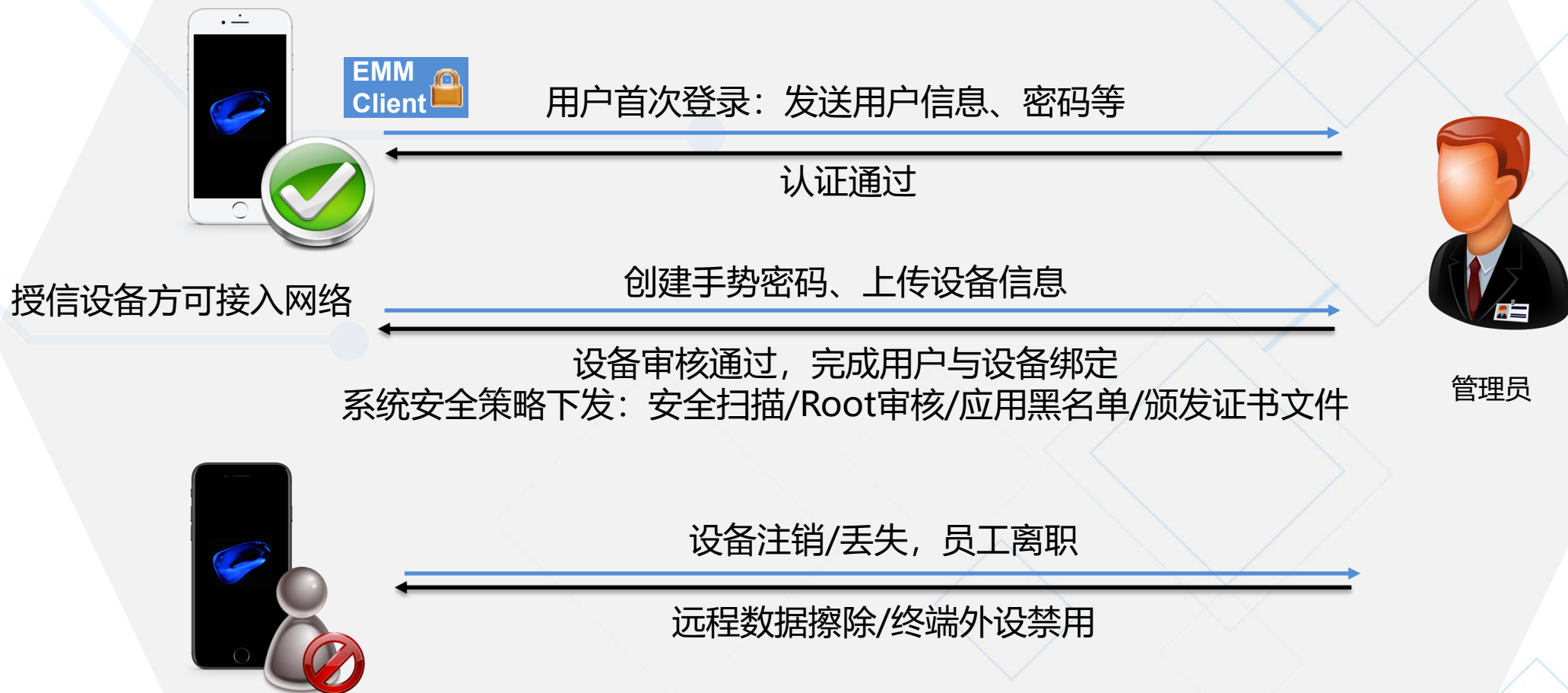
文档信息



帮助与反馈

设备管理——设备与用户绑定

用户与设备绑定，安全策略下发



设备管理 —— 管控力度，按需定义

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

• 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

基本信息

网络接口状态

关键进程信息

192.168.2.52

设备名称: localhost.localdomain

最近一次启动时间: 2019-11-18 15:57:48

运行时长: 3天19小时22分钟

磁盘性能: 空间利用率:

39%

总空间:31.41G 已使用:12.39G 剩余空间:18.2G

IO利用率:

读频率:0次/s 读速度:1K/s 写频率:1次/s 写速度:8.5K/s

CPU性能: 系统平均负载:最近1分钟:0.00 最近5分钟:0.01 最近15分钟:0.05

CPU使用率:

内存: 物理内存:

30%

内存大小:7.64G 已缓存空间:3.34G 已用空间:2.31G 剩余空间:1.99G

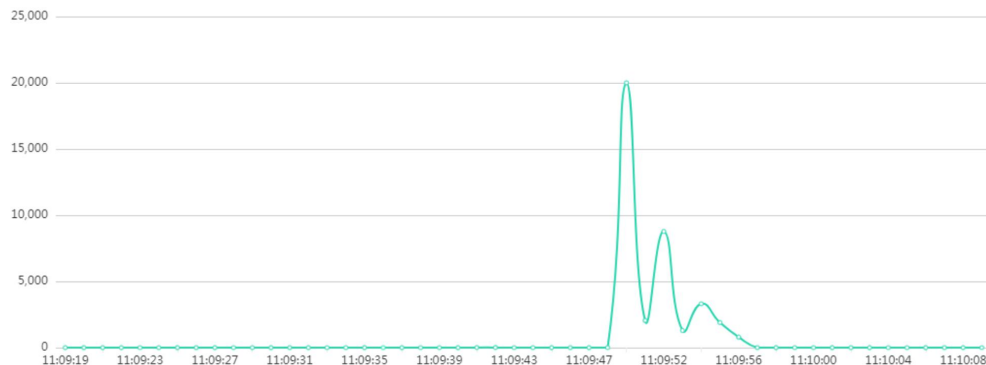
交换分区:

分区大小:2G 已用空间:0K 剩余空间:2G

192.168.2.55:9100

所有流量

流量 (KB)



运维管理——安全审计

- 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



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）

