中国移动
China Mobile

移动云SaaS产品介绍

www.10086.cn

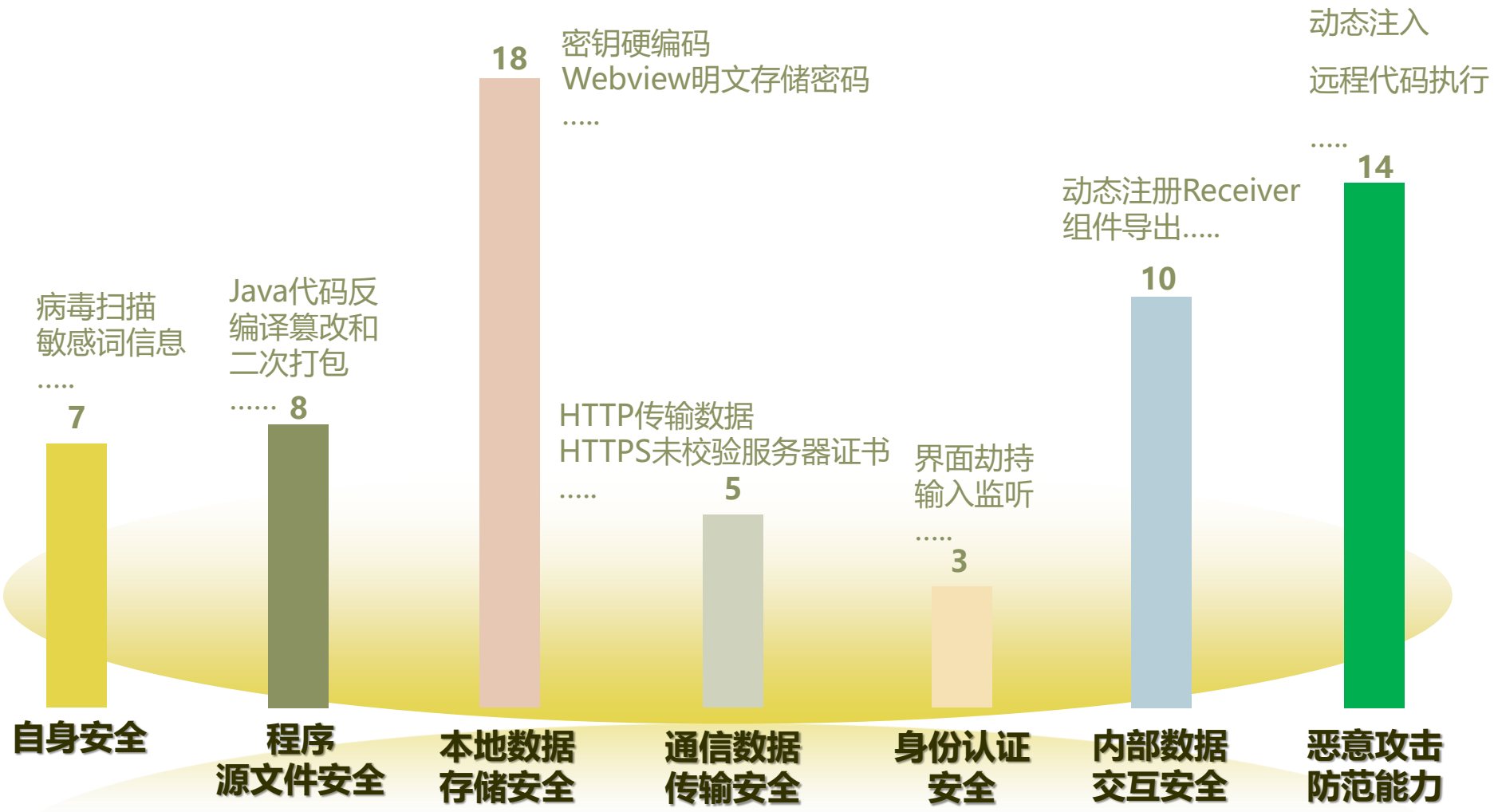
产品概述

移动测评云平台是什么？

以自动化的方式，全面、准确、高效的检测移动应用的安全性问题并提供修复方案

一、全面的自动化测评项目

全面的自动化测评项目，七个类别，Android共涵盖65个测评项目，iOS共涵盖26个测评项目



二、丰富的测评结果展示和报告输出

多种测评结果展示方式，多种形式的报告输出

在展示方式上

- 在线实时浏览测评结果
- Word和pdf两种格式的专业测评报告下载

在报告内容上

- 单个应用的测评结果详情、应用多个版本的分析报告、多个应用批量统计分析的测评结果
- 在测评结果修复建议中，包含代码级修复示例，可供开发者自主修复安全漏洞

二、丰富的测评结果展示和报告输出

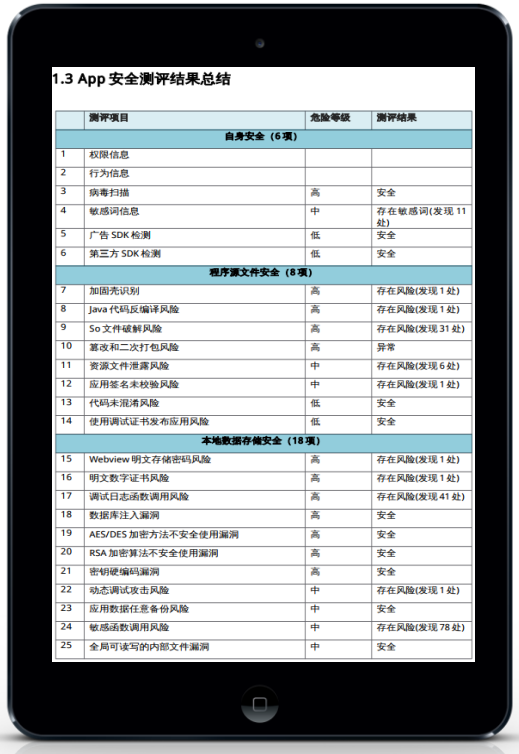
测评报告展示：App安全测评总览、App安全测评结果总结、测评项目详情（含代码级修复示例）

1 App 安全测评总览

1.1 App 测评得分

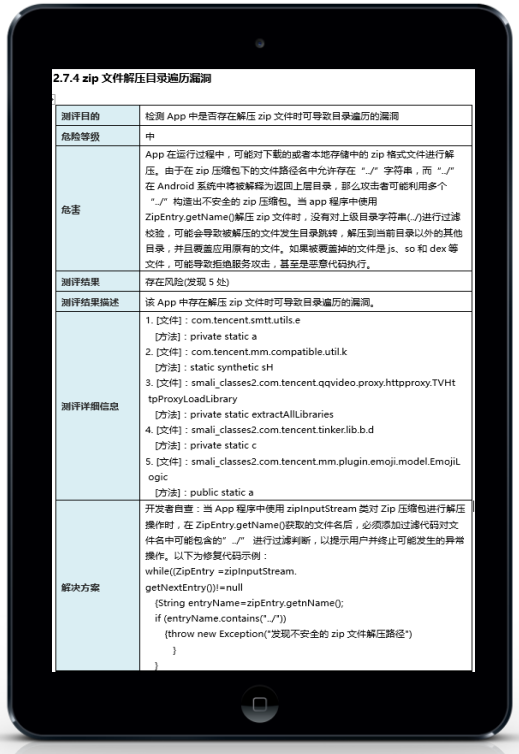
安全测评得分	47/100

	总计	高	中	低
测评项目数	64	19	24	21
存在问题测评项目数	33	11	15	7
发现问题	623	225	279	119



1.3 App 安全测评结果总结

	测评项目	危险等级	测评结果
	自身安全（6项）		
1	权限信息		
2	行为信息		
3	病毒扫描	高	安全
4	敏感词信息	中	存在敏感词(发现 11 处)
5	广告 SDK 检测	低	安全
6	第三方 SDK 检测	低	安全
	程序源文件安全（8项）		
7	加固壳识别	高	存在风险(发现 1 处)
8	Java 代码反编译风险	高	存在风险(发现 1 处)
9	So 文件破解风险	高	存在风险(发现 31 处)
10	篡改和二次打包风险	高	异常
11	资源文件泄露风险	中	存在风险(发现 6 处)
12	应用签名未校验风险	中	存在风险(发现 1 处)
13	代码未混淆风险	低	安全
14	使用调试证书发布应用风险	低	安全
	本地数据存储安全（18项）		
15	Webview 明文存储密码风险	高	存在风险(发现 1 处)
16	明文数字证书风险	高	存在风险(发现 1 处)
17	调试日志函数调用风险	高	存在风险(发现 41 处)
18	数据库注入漏洞	高	安全
19	AES/DES 加密方法不安全使用漏洞	高	安全
20	RSA 加密算法不安全使用漏洞	高	安全
21	密钥硬编码漏洞	高	安全
22	动态调试攻击风险	中	存在风险(发现 1 处)
23	应用数据任意备份风险	中	安全
24	敏感函数调用风险	中	存在风险(发现 78 处)
25	全局可读写的内部文件漏洞	中	安全



2.7.4 zip 文件解压目录遍历漏洞

测评目的	检测 App 中是否存在解压 zip 文件时可导致目录遍历的漏洞
危险等级	中
危害	App 在运行过程中，可能对下载的或者本地存储中的 zip 格式文件进行解压。由于在 zip 压缩包下的文件路径名中允许存在 "../" 字符串，而 "../" 在 Android 系统中将被解释为返回上层目录，那么攻击者可能利用多个 "../" 构造出不安全的 zip 压缩包。当 app 程序中使用 ZipEntry.getName()解压 zip 文件时，没有对上级目录字符串(../)进行过滤校验，可能会导致被解压的文件发生目录跳转，解压到当前目录以外的其他目录，并且覆盖应用原有的文件。如果被覆盖掉的文件是 js、so 和 dex 等文件，可能导致拒绝服务攻击，甚至是恶意代码执行。
测评结果	存在风险(发现 5 处)
测评结果描述	该 App 中存在解压 zip 文件时可导致目录遍历的漏洞。
测评详细信息	1. [文件]：com.tencent.smtt.utils.e [方法]：private static a 2. [文件]：com.tencent.mm.compatible.util.k [方法]：static synthetic sH 3. [文件]：smali_classes2.com.tencent.qqvideo.proxy.httpproxy.TVHttpProxyLoadLibrary [方法]：private static extractAllLibraries 4. [文件]：smali_classes2.com.tencent.tinker.lib.b.d [方法]：private static c 5. [文件]：smali_classes2.com.tencent.mm.plugin.emoji.model.EmojiLogic [方法]：public static a

解决方案	开发者自查：当 App 程序中使用 zipInputStream 类对 Zip 压缩包进行解压操作时，在 ZipEntry.getName()获取的文件名后，必须添加过滤代码对文件名中可能包含的"../"进行过滤判断，以提示用户并终止可能发生的异常操作。以下为修复代码示例：
	while((ZipEntry =zipInputStream.getNextEntry())!=null
	{String entryName=zipEntry.getnName();
	if (entryName.contains("../"))
	{throw new Exception("发现不安全的 zip 文件解压路径")
	}
	}

三、批量统计和数据统计

区别：批量统计——基于多个应用的统计分析报告；数据统计——基于所有测评数据的图表分析

数据统计

对象：测评结果列表中的应用

操作：左侧导航栏点击“数量统计”即可

内容：从“测评应用”和“测评项目”两个维度进行安全问题的统计分析

结果呈现方式：**在线实时统计图表呈现**

批量统计

对象：测评结果列表中的应用

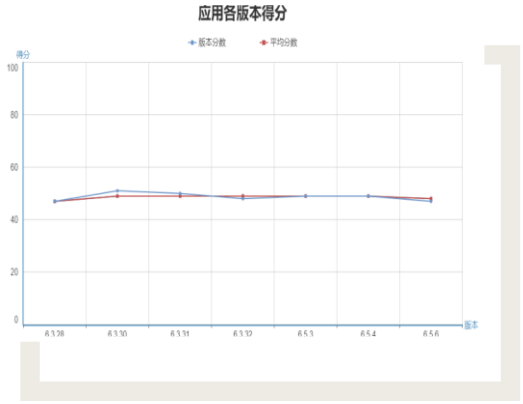
操作：在测评结果列表勾选多个应用——点击“批量统计”——下载批量统计报告

结果呈现方式：**直接输出批量统计报告**

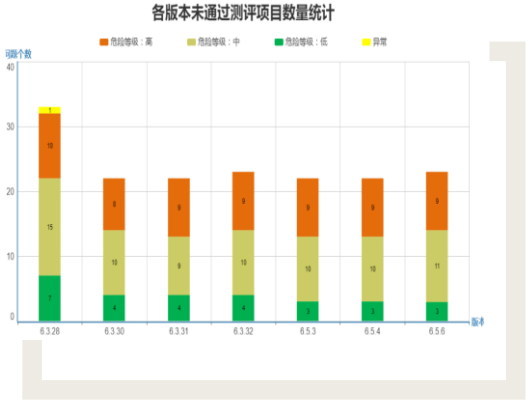
四、版本管理功能

可对应用的多个版本自动化关联及统计，实现版本自动化管理

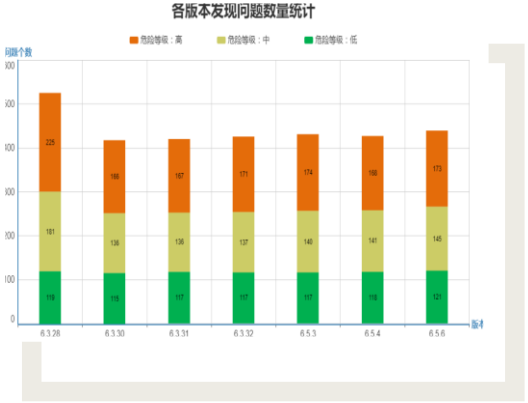
版本管理入口



应用各版本得分



各版本未通过测评项目数量统计



各版本发现问题数量统计

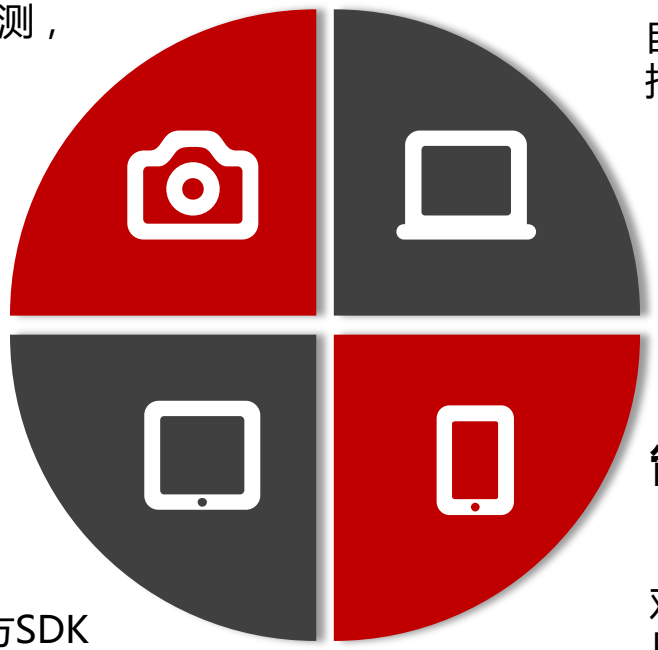
五、我们的特色功能

Android iOS 合二为一

同平台实现android和iOS检测，
可单独交付

检测结果可编辑

自主忽略风险项目
报告结果同步更新



第三方SDK安全问题单独呈现（Android）

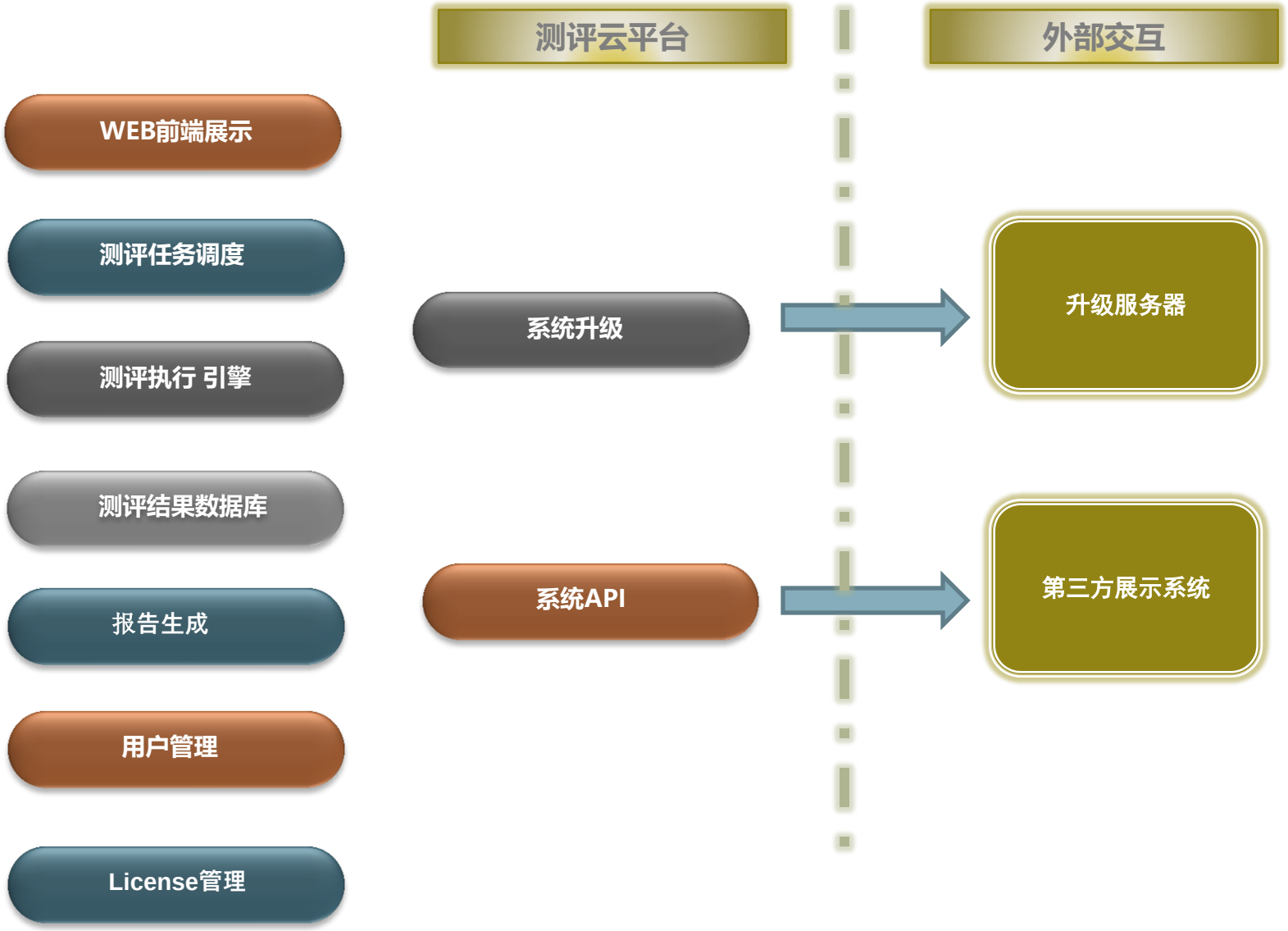
移动应用安全问题排除第三方SDK

管理员白名单管理（Android）

对SO文件、资源文件和调试日志函数进行管理；
全局白名单管理

技术架构

梆梆移动应用安全测评云平台功能模块拆解



产品特点


测评平台
六大亮点
国内首个突破60+检测项的移动应用测评云平台
测评平台新版本的测评项目从原来的46项增加到65项，国内同类产品中数量领先
检测结果的准确性程度领先
检测项目的检测结果在竞品中准确性最高，并可提供准确的安全问题定位。
国内领先结合静态技术和动态技术进行自动化测评
行业内，领先使用静态检测技术和动态检测技术相结合的方式实现自动化检测，国内大多同类产品仅采用静态技术。
可实现海量应用安全数据统计的移动应用测评云平台
支持测评应用安全性问题的数据统计，呈现安全漏洞检出分析图表
具备代码级修复示例的移动应用测评云平台
国内唯一具备代码级修复示例的移动应用测评云平台，供开发者快速自查和修复
支持版本安全性管理的移动应用测评云平台
可自动关联应用的多个版本，对版本进行安全性统计，清晰地呈现移动应用迭代过程中的安全性变化，并输出专业的分析报告内容

应用场景

应用场景-测评机构

- **客户类型**：测评机构、应用安全评估单位
- **客户需求**：对送检的大量应用进行测评
- **产品契合点**：测评项目覆盖当前主流安全问题、自动化的测评可有效快速处理大量的测评需求、可独立部署保障数据隐秘性

应用场景-监管机构

- **客户类型**：信息安全监管机构
- **客户需求**：对市场中的某类或某个行业应用中的安全问题进行分析统计
- **产品契合点**：行业类型应用数量巨大，需要自动化的解决方案；可提供调用接口，测评系统完成核心的安全问题测评，向客户返回测评结果和统计数据；可配合渠道监测系统进行大数据的收集分析

应用场景-银行等大企业

- **客户类型**：银行等大企业，旗下有多个应用
- **客户需求**：对旗下多个应用进行测评、修复以提高其安全性并保障其合规性
- **产品契合点**：快速的自动化测评系统可保障持续进行版本测试、迭代；独立部署，保障应用代码安全性；测评项目可根据需求快速定制

应用场景-中小企业及个人开发者

- **客户类型**：中小企业及个人开发者
- **客户需求**：对开发的应用进行测评、修复以提高其安全性；实现应用版本迭代的安全性管理；无法负担独立部署或维护安全团队的开销
- **产品契合点**：开通在线测评云平台使用账号，费用较低；可接受账户使用期限及可测评个数限制；测评项目覆盖当前主流安全问题，准确定位并且提供修复方案；提供应用版本迭代过程中的安全问题自动化管理

售后支持

服务目标：快速响应、高效处理
服务宗旨：专注、规范、卓越

1、专业团队帮助客户进行权威的检测报告解读；

2、系统版本客户透明化升级；

热线电话：4008-881-881
专属在线QQ 通道：1462274966
客服邮箱：service@bangcle.com
专属售后技术邮箱：support@bangcle.com

客户案例

大型企业：银行、互金、券商、运营商等

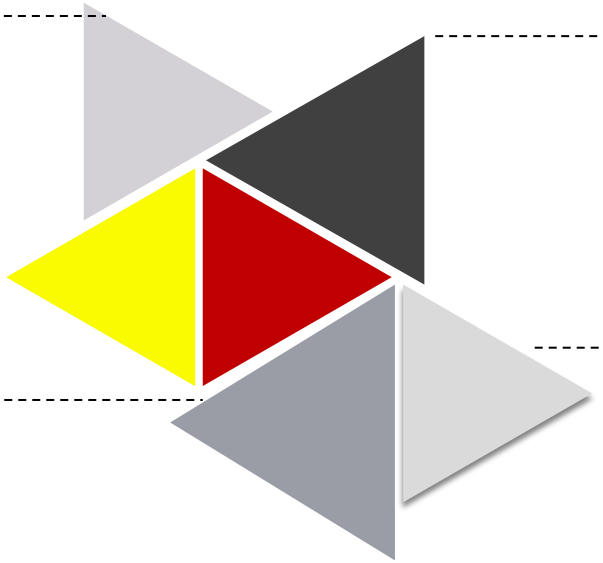
保障自身移动应用的安全
建立行业内的移动应用安全标准（行业领头）
满足行业内更高级别的监管要求

参考案例：中国银行、农行——银行
东方证券，中信证券——券商
中国移动多个地区分公司

测评机构/监管机构

提升自身移动安全检测能力及效率
提供移动应用安全检测报告及整改建议

参考案例：公安部第三研究所、CNCERT
中国信息安全测评中心
中国信息安全认证中心
广州、上海、深圳测评中心



政府部门、政企单位（含电力等）

需要保障体系内App的安全；
建立自身体系内的移动应用安全标准

参考案例：中国电力科学研究院
上海电力研究院
湖南电子信息产业研究院
福建省、北京电力科学院

其他企业、个人开发者

保障自身移动应用的安全
提升自我安全修复能力
保障上架应用安全

参考案例： 新东方
唯品会

中国移动
China Mobile

谢谢！