ASC

应用安全联盟

2016 移动物联网安全高峰论坛

移动应用安全新技术

通付盾 华保健

目 录
CONTENT

APP安全问题严重

盗版应用猖獗，手游是盗版应用重灾区

性格测试、算命、假红包等恶意链接窃取隐私

社交软件隐私泄露频发

移动端支付财产安全问题令人担忧

某SDK涉嫌窃取用户信息涉及多款APP从苹果下架

应用内信息泄露，数据泄露危害严重

XcodeGhost时间敲响开发者警钟

APP开发者版权安全需保护

钓鱼网站危害惊人

伪基站发送钓鱼网址，诈骗短信冒充银行问题严重

吸费吸流量问题严重

央视曝出多家主流手机的流量偷跑问题

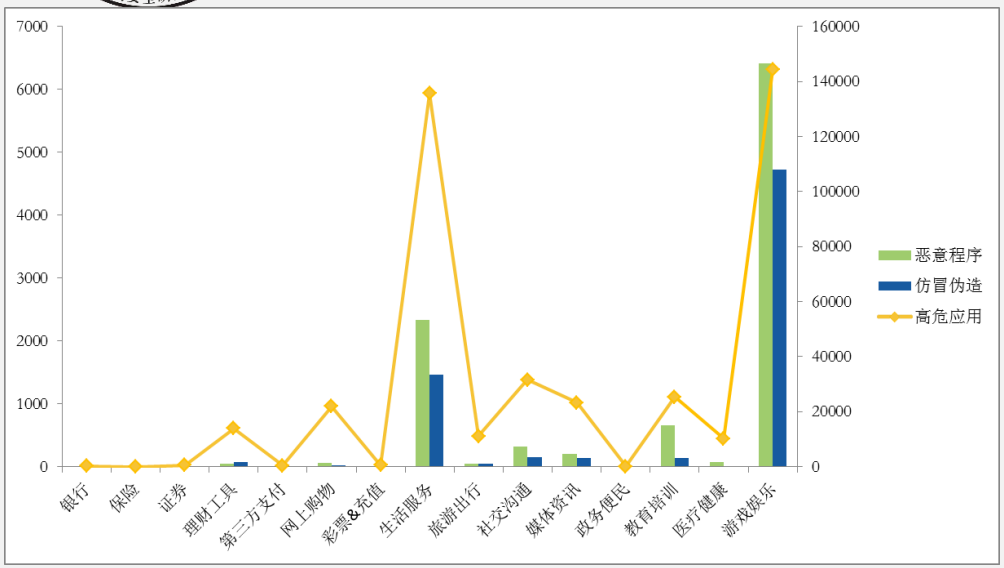
公共WiFi泄露信息

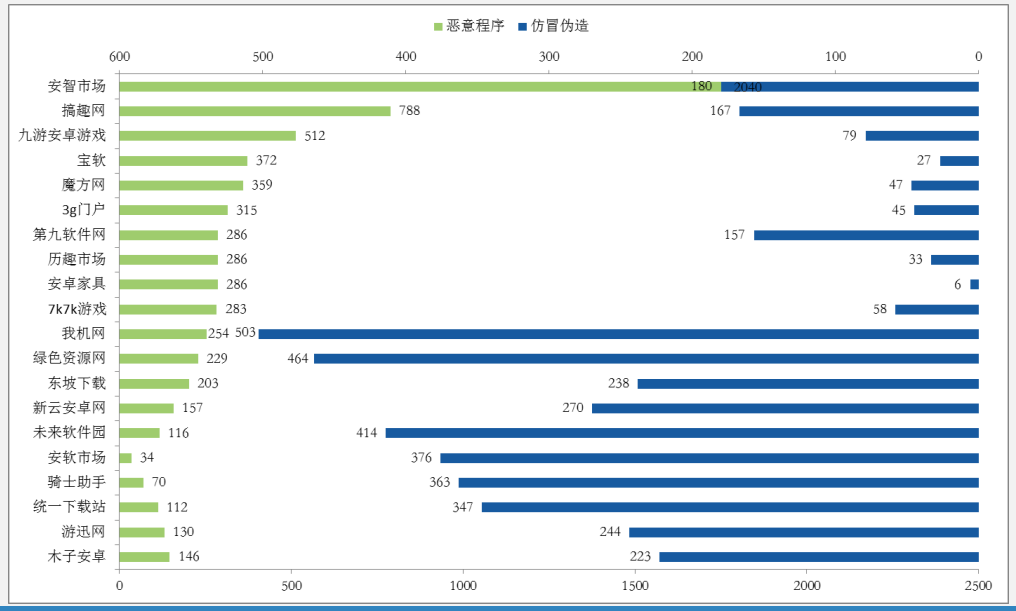
手机转卖遭遇信息泄露

病毒、恶意扣费类软件猖獗

手机APP被植入恶意代码问题严重

APP安全现状





通过对全网**近300**家应用市场，**320万**移动应用的监测，仅2016年第三季度通付盾移动应用监测平台安全监测结果如下。

截获17,002个恶意应用，7,264个仿冒伪造应用，534,800个高危应用，危险应用占全网应用的比例为26.54%，即每10个应用中有近3个危险应用，用户的隐私、财产面临重大的安全隐患。

截获仿冒伪造应用7,264个，游戏娱乐行业仿冒伪造应用占比最高，其次为生活服务和社交沟通行业。

发现高危漏洞534,800个，多集中于生活服务、游戏娱乐、媒体资讯行业。

从地域分布来看，危险应用（包括恶意程序应用、仿冒伪造应用、高危漏洞应用）最多的地区是**北京、广东**两个应用市场数量最多的省市。**北京、广东、湖北、福建、上海**这五个城市发现恶意程序、仿冒伪造、高危漏洞的次数均较多，属于危险应用的高发地带。

要求和规范

2013年

2014年初，成立两个国家级安全机构：国安委、中央网络安全与信息化领导组习总亲自挂帅

2014年

2014年5月，国家互联网信息办宣布，我国将推出网络安全审查制度

2014年5月，公安部发布《信息安全技术信息系统安全等级保护基本要求 移动互联要求标准草案》，明确要求移动安全等级保护工作

2014年8月，工信部发布《关于加强电信和互联网行业网络安全工作的指导意见》，进一步强化移动互联网的安全管理工作

2015年

2016年

2016年8月1日，国家网信办发布的《移动互联网应用程序信息服务管理规定》正式执行，加强对应用程序提供者和互联网应用商店的监管

01

APP安全加固新技术

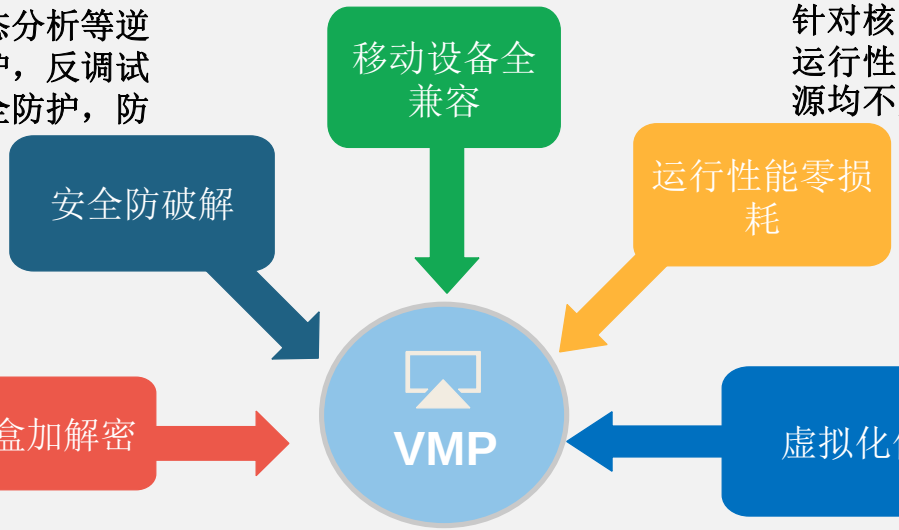
应用加固产品对抗移动应用逆向工程、二次打包、代码注入等攻击行为，为企业App服务，提高企业App安全性。

APP加固新技术

VMP保护完全不影响原程序的兼容性，完美适配Android/IOS不同系统版本和设备。

对抗脱壳、静态分析、动态分析等逆向工程手段，进行内存保护，反调试保护，本地数据加密等安全防护，防止应用被破解。

针对核心函数做保护，不影响程序运行性能，应用响应速度和使用资源均不受影响。



通过白盒加解密技术，使用数学运算替代密钥，加密过程更安全。

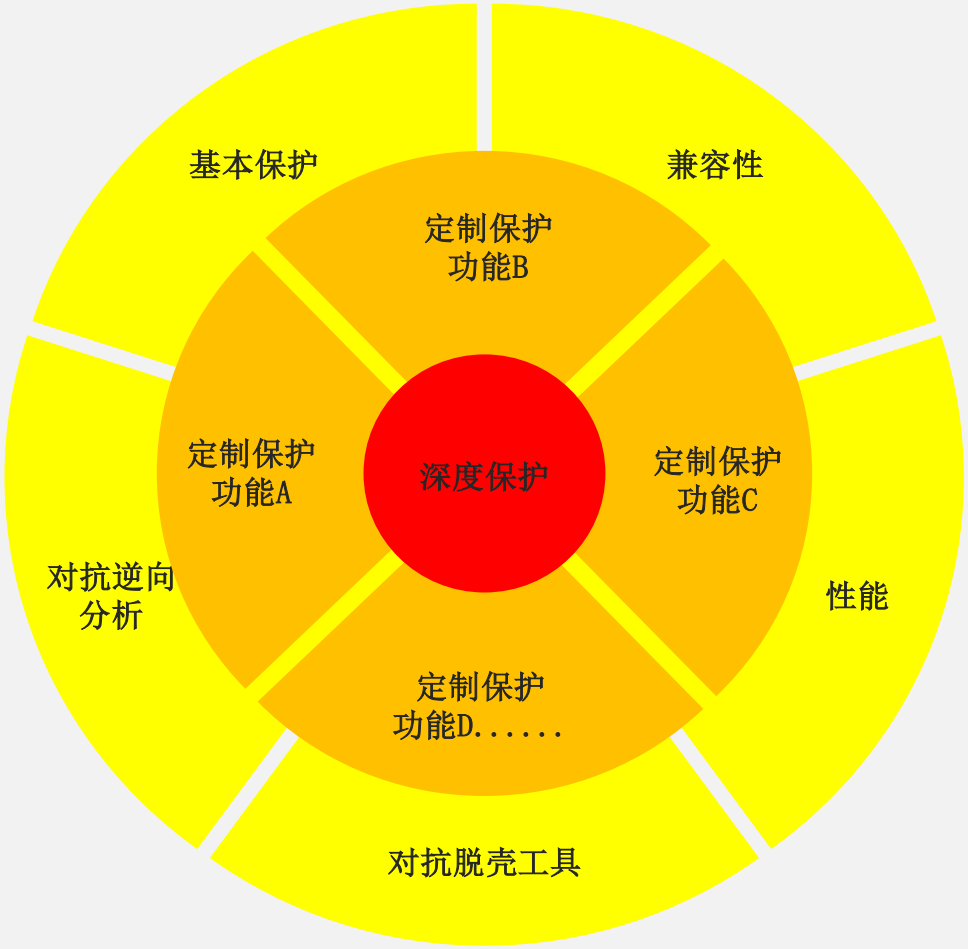
虚拟机保护（VMP）是业界公认强度最高的应用保护方案。

PC时代的VMProtect由俄罗斯人发明，是一种安全强度极高的软件加固系统，虚拟机保护技术也成为业界公认保护强度最高的软件加固方案之一，至今未被破解。

通付盾推出的通付盾VMP是国内独家真正将虚拟机保护技术使用在移动应用加固领域的厂商，应用加固进入“移动设备全兼容、运行性能零损耗、安全防破解”的新时代。

通付盾VMP不同于友商基于“函数功能隐藏”、“代码混淆”的伪VMP保护方案。

APP加固服务



标准版

整体加固，基本保护，优先保证兼容性和性能。

特点：稳定性高，满足合规要求。

增强版

在标准版的基础上提供多种其他保护功能，满足不同客户加固需求。

特点：功能丰富，满足不同客户的加固需求。

高级版

在增强版的基础上提供定制和深度防护，安全性最高，定制性最强。

特点：深度保护，定制服务。

优势

移动设备全兼容

加固算法采用在所有Android系统版本都共有的API；VMP保护兼容ARM、x86等各CPU架构。

运行性能零损耗

加固阶段通过硬件虚拟化技术将部分高级语言（c/c++等）和汇编指令优化成机器指令，性能无损耗。

安全防破解

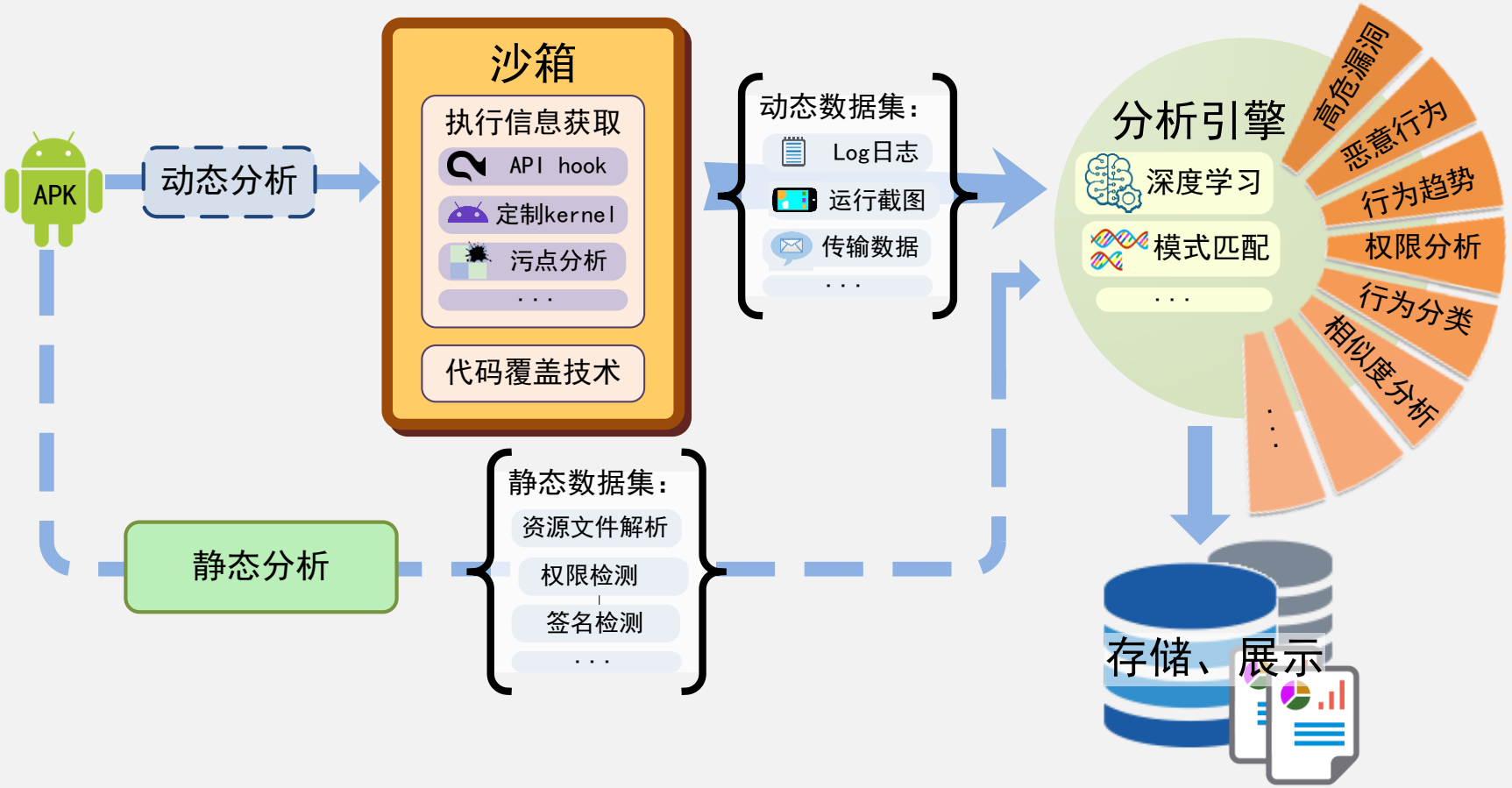
采用整体加固和关键功能重点保护（VMP）相结合的方案，大大提高移动应用安全性。

02

APP安全检测

对APP进行动静结合的双擎检测，全面发掘APP安全问题。

双擎扫描



通付盾移动应用安全检测产品是对APK文件（Android）进行全方位**动静结合**的安全检测，在上架前帮助企业发现应用安全问题，及时修复。

检测报告

- 案例仅供参考


漏洞分布

漏洞详情

01应用层

中危 签名校验

低危 Activity安全

低危 Receiver安全

低危 Debug安全

低危 本地拒绝服务

安全 硬编码安全

安全 AllowBackup

安全 随机数使用

安全 Wormhole

02网络传输层

中危 通信协议安全

安全 SSL中间人攻

低危(7个

Log记录安全			
分析结果	高危	等级分布	高危 7;中危 0;低危 0
漏洞描述	Log信息泄露程序运行逻辑或用户敏感数据，降低逆向分析的难度和增加用户隐私被窃取的风险。		
修复建议	去除不必要的Log信息。		

漏洞编号	威胁等级	漏洞明细
11-0001	高危	Lcom/shoujiduoduo/ui/cailing/GiveCailingActivity;->onActivityResult (IILandroid/content/Intent;)V|Lcom/shoujiduoduo/base/a/a;->a(Ljava/lang/String; Ljava/lang/String;)V|Lcom/shoujiduoduo/base/a/b;->b(Ljava/lang/String; Ljava/lang/String;)I|Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

优势

三大核心优势

双引擎扫描

动态分析和**静态分析**双擎扫描。全面发现App安全问题。

深度学习

基于**深度学习**的病毒扫描和漏洞挖掘引擎，技术领先。

APP安全大数据

基于**全网全量**APP准实时扫描，形成移动安全大数据，不断修正和完善检测规则和模型。

03

APP安全监测

覆盖全国各应用市场，实时监测全网数百万APP安全状况。

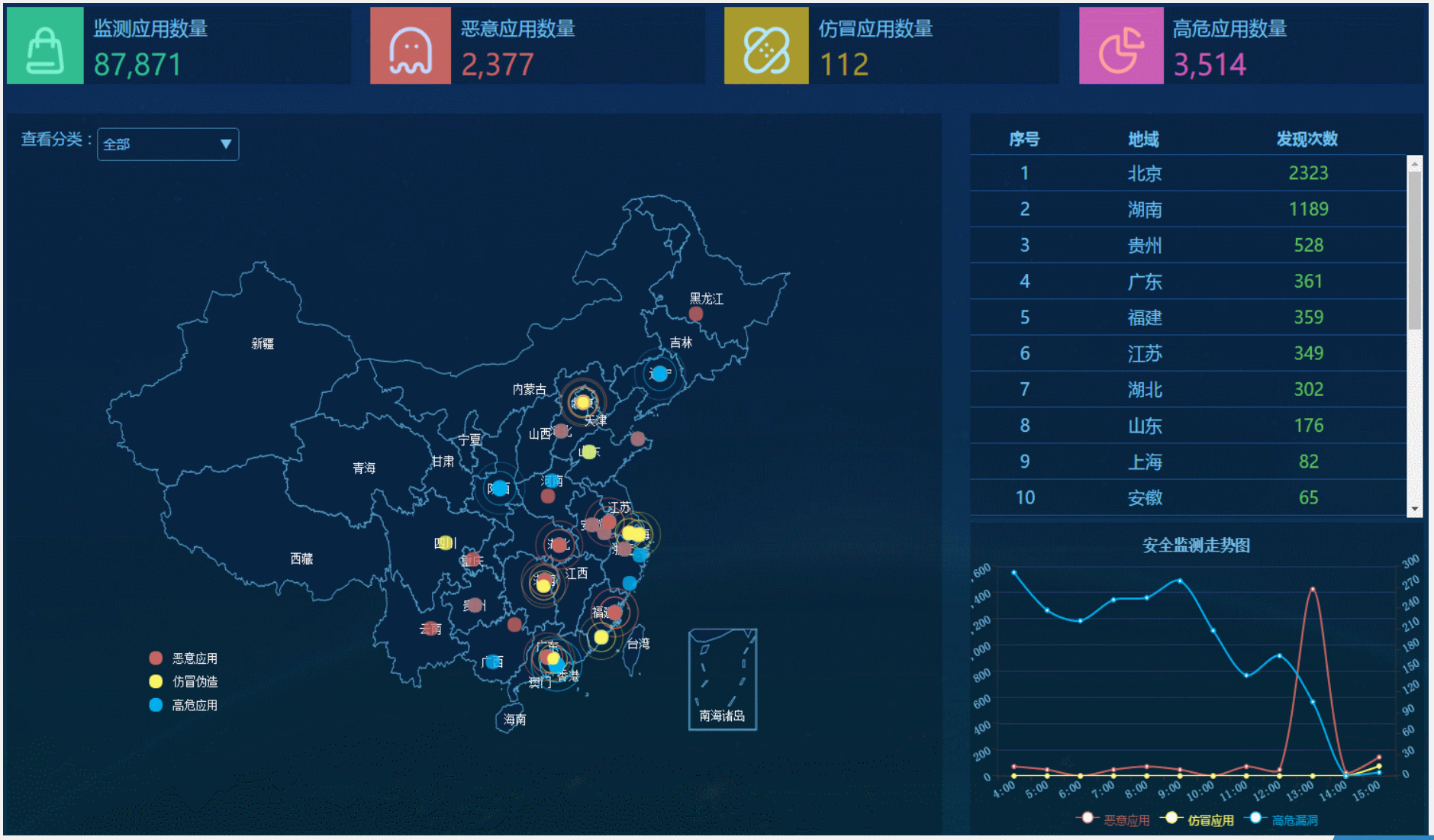
APP安全大数据

覆盖全国所有移动应用分发渠道

数据准实时更新，7*24无间断监测

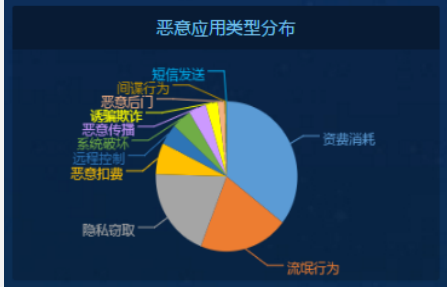
APP安全大数据是通过对全网所有APP的爬取、分析、统计和不断更新，形成实时准确反映全网APP安全态势，可助力移动应用安全监测和管理的大数据平台。目前，我国本土共有**300多家**第三方移动应用商店，应用数量累计达到**371万**，用户规模**超8亿**。

实时监测：准实时掌握全网应用安全状况



覆盖近300应用市场，数百万全网APP全量安全状况数据统计分析。

渠道市场数量	监测应用数量	恶意应用数量	仿冒应用数量	高危应用数量
248	1,938,824	15,639	7,264	498,504



序号	地域	危险应用发现次数
6	上海	40,646
7	山东	32,223
8	江苏	31,713
9	贵州	23,193
10	浙江	19,251
11	河北	11,964
12	安徽	9,406
13	陕西	4,543
14	河南	4,541
15	四川	3,542
16	辽宁	2,090
17	香港	1,961
18	山西	1,470
19	重庆	960
20	天津	748
21	黑龙江	568
22	广西	439
23	云南	7
24	江西	1

优势

数据全

覆盖**全网**各应用市场，**数百万APP**，持续更新，全量爬取、全量分析。

准实时

准实时更新APP安全数据，TOP20应用市场**每小时**更新，其他市场**每日**更新。

多维度

从**行业、渠道、地域分布**等多个维度全面分析应用安全状况，独家集合**漏洞挖掘**、**病毒检测**，**仿冒应用监测**，**内容违规识别**四大引擎。

精度高

基于**动静结合**的自研深度程序分析引擎DeepScan和**机器学习**技术，数据准确有效。

建议

一、APP发展迅猛，安全保障必须重视，在加强对移APP开发者、应用市场监管中，APP安全大数据是最有效手段。

二、广泛推广使用APP安全新技术，应对不断变化的移动安全新形势，实现应用加固“移动设备全兼容、性能零损耗、安全防破解”的客观需要。上线前进行安全检测，防止“带病上线”是安全需求。

三、关注通付盾移动安全实验室，官方微信公众号：“通付盾移动安全”，扫码关注 ☺☺☺：

谢 谢！