iResearch
艾 瑞 咨 询

中国移动应用安全服务行业白皮书

2017年

开篇摘要

发展驱动力

- 移动应用安全市场整体处于发展初期阶段。
- 移动应用安全市场发展主要驱动力：其一，政策落地，对移动应用市场的安全等问题作出明确规定；其二，市场恶意软件泛滥，为移动应用安全防护市场带来机遇；其三，移动网民的持续增加与移动生活在在人们生活的不断渗透推动移动应用安全市场发展。

市场发展

- 安全检测：人工渗透测试和自动化检测是目前常用的两种检测手段。
- 安全加固：将dex文件进行加密处理，并将目标程序的入口指向壳程序是dex文件加固的原理，目前的加固技术是初级加固技术与虚拟机加固技术配合进行。
- 安全监测：渠道管理、识别仿冒程序以及大数据分析是安全监测的常用手段。

市场格局

- 国内移动应用安全市场中，主要存在互联网企业背景和垂直移动安全企业两大类主要玩家。
- 移动应用安全市场集中度相对偏高，中等偏大企业进入市场较早，客户群体覆盖比较广，但整个市场的准入度较高。
- 移动应用安全市场未来将在复杂应用的加固保护方案和恶意应用攻击向底层渗透这两个方面发力。

发展趋势

- 人工智能、机器学习将深度应用至安全检测，有效提升安全检测的质量与效率。
- 移动应用安全企业开始注重安全服务生态圈，安全服务将覆盖至整个产业链上下游。

艾瑞研究院自主研究绘制。

定义

针对移动应用生命周期可能出现的隐患提供的解决方案

目前业界还没有针对移动应用安全服务给出权威的定义，本文的移动应用安全服务指的是针对移动应用的开发、发布、分发以及安装使用等全生命周期阶段提供的开发咨询服务、安全咨询及安全保障等服务。

移动应用开发的生命周期的简单示意图

开发者

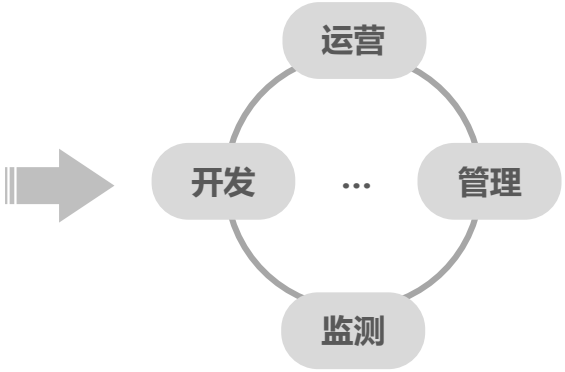
移动应用开发者在开发者平台上开发应用并将最终开发好的应用发布到各应用商店。

应用商店

应用商店将开发者开发的应用整合分类，并利用分发渠道将开发者发布的应用分发/推送给用户。

用户

用户从应用商店或者官网上下载应用，并安装应用。



提供安全服务的各个方面

来源：艾瑞研究院自主研究绘制。

Android平台的结构及特点

平台整体为层次结构，且各层功能分明

Android移动设备平台的软件层次结构自上而下分别为：Application（应用程序）、 Application Fraework（应用程序框架层）、系统运行是的各种类库和Android运行环境层以及Linux Kernel（Linux内核层）。其中Dalvik虚拟机位于安卓运行环境中，它主要是通过解释dex文件来执行由Java字节码转换而来的Davilk字节码，从而达到运行Android程序的作用。

Android平台系统架构图

来源：艾瑞研究院自主研究绘制。

Android平台的不足

平台架构及运营模式的不足造成移动应用安全受威胁

虽然Android平台本身有比较规范的安全机制，如应用层引用签名机制、应用权限控制机制保护程序的安全；内核层通过沙箱机制隔离不同进程的资源，并辅助独特的内存管理机制和进程间通信机制等。但是由于Android本身的开源性、推广的开放性等因素，安卓平台在自身架构、架构的安全机制以及平台的运营模式等方面均存在一定的不足，这些问题一旦被攻击者利用，用户的利益将受到侵害。

Android平台的不足

平台架构

Linux提权攻击风险

Root是Linux的最高权限，攻击者一旦拥有Root权限就可以对系统和文件进行肆意修改。

非法系统篡改

原生Android系统缺乏对系统镜像加载过程的安全防护，攻击者可以在系统内植入或安装非法程序。

APK逆向破解

Android采用Dalvik虚拟机进行代码执行，由于解释语言的机制会导致Android应用容易被攻击者通过反编译的手段进行逆向分析，进而恶意修改代码后二次打包，损害用户利益。

安全机制

伪造应用签名

Android的签名机制保证应用的安全性，但今年来暴露的签名漏洞使得攻击者利用恶意程序伪造合法应用而绕过验证机制。

模糊的权限声明

用户安装应用时无法通过阅读权限说明明确应用的真实意图，进而无法对用户决策产生有效支持。

作用受限的数据保护机制

Android仅采用了基于文件系统的加密技术保障数据安全，一旦设备正常运行，数据将暴露与系统的明文空间内，则其数据保护作用将受限。

运营模式

版本碎片化

由于Android采用完全开源及开放的推广态度，故市场上运行的安卓版本众多。版本过度分散会导致系统漏洞修复迟滞，一旦谷歌停过之对某个版本前的漏洞修复，用户利益将受威胁。

第三方Rom良莠不齐

Android系统的开放性使得第三方Rom市场繁荣，但由于第三方Rom的水平良莠不齐，可能会导致系统漏洞暴露，给攻击者带来可乘之机。

应用市场多样化

用户主要从第三方应用市场下载应用，而Android应用市场多，且缺乏审核监管机制，因此恶意软件泛滥，Android生态环境较差。

来源：艾瑞研究院自主研究绘制。

移动应用安全所处的政策驱动力

政策助力移动应用安全行业发展规范化、制度化

移动互联网的发展和智能手机的普及使得手机上网越来越流行，移动互联网时代的爆发更是带动移动端设备趋于全能化的发展，而与此同时，手段安全隐患越来越多、问题越来越突出。因此从2016年全国人大、网信办、公安部、工信部出台了多条相关的法律法规，净化网络空间安全、打击网络违法犯罪，助力安全市场发展。

2017年中国移动应用安全行业的政策环境

法律法规	主要内容	主要意义
移动互联网应用程序信息服务管理规定 2016年8月1日起施行	主要涵盖了关键信息基础设施保护、网络数据和用户信息保护、网路安全应急与监测等领域，并加强了个人信息保护要求，加大了对网络诈骗等不法行为的打击力度。	首次明确了国家网信办作为移动应用程序信息服务的主管单位，针对应用程序市场中的问题，如过度收集用户信息、恶意扣费等安全问题，都给出了明确规定，加强了APP信息服务规范管理，使得网民利益遭受侵害时有法可依，且投诉便捷、高效。
关于促进移动互联网健康有序发展的意见 2017年1月1日起施行	完善了市场准入制度，提升网络安全保障水平，维护用户合法权益、打击网络违法犯罪、增强网络管理能力，防范移动互联网安全风险。	《意见》提到将加大对移动互联网技术、商业模式等创新成果的知识产权保护，研究完善法律法规，规范网络服务秩序，提高侵权代价和违法成本；对完善移动互联网用户信息保护制度，严格规范个人信息收集，严查造谣诽谤等行为。
中华人民共和国网络安全法 2017年6月1日起施行	主要涵盖了关键信息基础设施保护、网络数据和用户信息保护、网路安全应急与监测等领域，并加强了个人信息保护要求，加大了对网络诈骗等不法行为的打击力度。	构建了我国首部网路空间管辖的基本法律法规，网络参与者提供普遍法律准则和依据，推动全社会网络安全意识的提升和网络安全保障水平的发展。

来源：艾瑞研究院自主研究绘制。

移动应用安全所处市场驱动力

市场恶意软件泛滥，移动应用安全市场亟待解决

根据《YD/T2439-2012移动互联网恶意程序性描述格式》，移动互联网恶意程序行为属性包含以下8类：恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。

2017年中国移动应用常见的恶意软件分类及其行为

恶意扣费 在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失。

在用户不知情或未授权的情况下，获取涉及用户个人隐私信息的行为。 **信息窃取**

远程控制 在用户不知情或未授权的情况下，能够接受远程控制端指令并进行相关操作。

自动通过复制、感染、投递、下载等方式将自身、自身衍生物或其他恶意代码进行扩散。 **恶意传播**

资费消耗 在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁链接网络等方式，导致用户资费损失。

通过感染、劫持、篡改、删除、终止进程等手段导致移动弄终端或其他非恶意软件部分或全部功能、用户文件等无法正常使用的，干扰、破坏、阻断一段通信网络、网络服务或其他合法业务正常运行。 **系统破坏**

诱骗欺诈 通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱骗用户而达到不正当目的。

执行对系统没有直接损害，也不对用户个人信息、资费造成侵害的其他恶意行为。 **流氓行为**

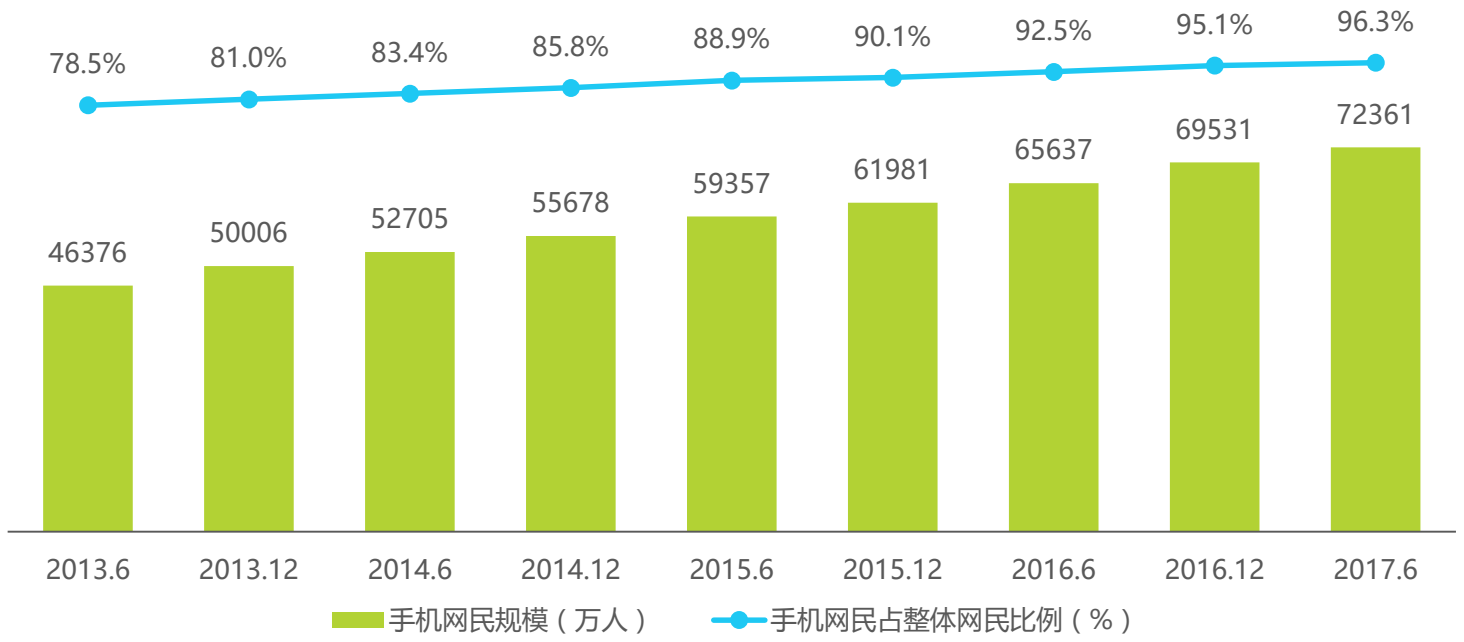
来源：艾瑞研究院自主研究绘制。

移动应用安全所处的社会驱动力

移动基础设施的普及和移动生活的便利性共促行业发展

截至2017年6月，我国手机网民规模达7.24亿，较2016年底增加2830万人。网民使用手机上网的比例有2016年底的95.1%提升至96.3%。移动网民的增加，尤其是移动化生活逐步渗透至人民的金融消费、出行、教育、娱乐等各领域，因此移动网民对移动应用的安全性和安全强度将会提出新的要求，促使移动应用安全企业持续研发更新新的安全防护技术，加速移动应用安全市场的发展。

2017年中国手机网民规模及其占整体网民的比例



来源：CNNIC第40次《中国互联网络发展统计报告》。

Android平台移动应用程序的结构

dex文件是移动应用程序的核心，也是被重点攻击的对象

Android平台应用发布时会打包成APK（Android Package，安卓安装包）文件，用于传输至终端设备安装，该文件是一个格式为ZIP的压缩包，里面包含配置文件、二进制代码、资源文件等众多文件。其中AndroidManifest文件是一个描述Android应用的“整体内容”的设定文件；META-INF目录则是应用程序完整性的第一道保护墙；classes.dex文件是可执行文件，保证应用得以在Android平台运行。从软件结构来看，当恶意代码植入应用中时，只需修改相应配置文件、启动组件等，就能让恶意代码伴随正常软件运行，进而为用户带来威胁。因此针对移动应用的安全防护势在必行。

Android平台移动应用程序的结构及其对应的功能

AndroidManifest.xml 应用配置文件	程序的全局配置文件，相当于Android应用向Android系统“自我介绍”的配置文件。
META-INF 存放应用程序签名和证书	META-INF目录下存放的是签名信息，用来验证APK文件的完整性和系统的安全性。
classes.dex Dalvik字节码代码文件	Dalvik字节码，承载源程序class的业务逻辑。
res目录 存放应用程序的资源	存放所有的资源文件，这些文件包括应用所使用的字符串常量、不同分辨率的图片和布局文件等。
lib目录 程序依赖的native库	存放第三方库文件，供应用调用第三方开源库。
resources.arsc 资源配置文件	编译后的二进制资源文件。

- classes.dex是文件运行的核心，并且在Dalvik字节码文件中保留大量的源代码信息，是攻击者攻击的重点对象。
- Android应用的关键代码可通过C或C++语音编写的SO库实现，而SO库的破解方法与工具在不断升级，故SO库保护十分必要。
- META-INF是应用程序得以安装的第一道屏障，需要防止签名信息被篡改或盗取。

来源：艾瑞研究院自主研究绘制。

移动应用常见的攻击类型

逆向分析、篡改等是移动应用常见的攻击类型

现阶段，权限滥用、逆向分析、二次打包及篡改等是Android平台应用最为常见的攻击类型，一旦发生，会导致用户的隐私等发生泄漏，对用户的切身利益等带来风险。其中逆向分析对移动应用的攻击不但会损害用户的利益，而且可以将核心的算法用于攻击者自己的程序中，侵害攻击者的知识产权。

2017年中国移动应用常见的攻击类型

权限滥用

通过声明过多的应用权限，安卓应用可以对用户本地文件、蓝牙设备等进行操作，如发送短信、连接网络等，在用户不知情的状态下窃取用户的个人隐私。

逆向分析

通过对应用的逆向分析，可发现应用中的核心算法或敏感信息，得知程序的逻辑、流程等，从而绕过用户应用中心使用的认证、加密手段，并插入恶意代码，给用户使用造成风险。同时还可能会将核心算法用于自己的程序中，侵害开发者的知识产权。

二次打包

二次打包是近年来恶意软件实施攻击的抓哟方式，通过将自身代码加在合法应用代码中，通过绕过Android的应用签名机制使应用正常安装，用户一旦使用，可能会遭受广告弹窗、信息劫持等安全风险。

篡改

攻击者通过逆向分析了解了程序的执行流程或者直接获得程序的源码，针对程序运行中的逻辑代码进行修改，绕过程序的验证保护机制，从而实现破解程序的目的。根据篡改方式的不同，一般可以分为静态篡改和动态篡改两类。

来源：艾瑞研究院自主研究绘制。

PC端和移动端遭受攻击区别

PC端攻击对象多为企业，移动端攻击对象普遍为用户

通常，PC端遭受的攻击对象主要是同过个人引向企业，而移动端遭受的攻击对象则主要是广大的移动端用户。随着移动终端在日常生活中的重要性愈发提升，针对移动终端的攻击能够获得高价值、高精度的信息，导致移动威胁攻击不可避免的向着长尾化、精准化和碎片化的方向发展。因此针对移动端的安全防护，除了用户自身要对连接的网络安全引起重视外，涉及移动应用生命周期的相关企业则需要对应用的开发、发布、分发等各阶段的安全负责，提升移动应用的生态安全环境。

2017年中国PC端和移动端遭受攻击的对比

	PC端	移动端
攻击类型	后门程序、信息炸弹、拒绝服务（分布式D.O.S攻击）、网络监听、DDOS（分布式拒绝服务）	权限滥用、逆向分析、二次打包、篡改
攻击对象	一般利用个人用户对企业进行攻击，而对个人攻击则主要是以勒索为主	攻击对象以普遍以用户为主
防护方法	更多依赖于杀毒软件	一方面对连接网络安全比较重视；另一方面则需要相关企业对APP的生命周期的安全负责。
加固产品通用性	相对较高	相对较低

来源：艾瑞研究院自主研究绘制。

移动应用常见安全防护手段

以加固为核心，检测和监测为主要辅助进行安全防护

由于移动应用安装包本身的结构特性和通过恶意攻击可能获取的利益关系，现阶段移动应用恶意软件泛滥，因此针对移动应用安全防护的服务开始出现。现阶段，针对移动应用的防护主要从安全检测、安全加固和安全监测三个方面着手，其中安全检测可以监测出应用可能存在的安全风险，具有安全预防作用；安全加固加固环节是移动应用最为直接有效的安全防护环节，有效预防攻击者的逆向、篡改、调试及窃取等行为；针对安全监测收集的各类应用数据的分析挖掘，可以有效识别有问题的应用，发出预警。目前移动应用安全防护企业正着力打造检测、加固、监测的服务闭环，提升移动应用的安全。

2017年中国移动应用常见安全防护类型

安全检测	安全加固	安全监测
通过自动化检测和人工渗透测试法对移动应用进行全面检测，并挖掘出系统源码中可能存在的安全风险、漏洞等问题，帮助开发者了解并提高其应用开发程序的安全性，有效预防可能存在的安全风险。	移动应用安全加固是针对移动应用普遍存在的破解、篡改、盗版、调试、数据窃取等各类安全风险提供的有效的安全防护手段，其核心加固技术主要包含防逆向、防篡改、防调试及防窃取这四大方面，不仅保护了APP自身安全，同时对APP的运行环境及业务场景提供了保护。	安全检测是通过对全网各类渠道的各类APP进行盗版仿冒、漏洞分布、恶意违规等方面的监测，分析监测收集的数据，精确识别出有问题的应用，并发出预警提示，同时将结果反馈给检测及防护环节，形成安全防护闭环。
安全预防	直接有效的安全防护	分析反馈并预警

来源：艾瑞研究院自主研究绘制。

安全防护手段-安全检测

人工渗透测试与自动化检测相结合提高检测精度与效率

现阶段Android移动应用程序的安全检测主要是针对移动应用程序的代码安全、组件安全等方面所做的安全检测服务，通过遍历程序执行路径，分析程序运行逻辑，检测因不规范编码引入的安全漏洞和使用不安全API及带有不安全的第三方SDK造成的危害。现阶段通行的主要有两种检测方法，分别为人工渗透检测和自动化检测。安全检测的目的主要是在应用上线前发现安全漏洞，将安全隐患提前找出，防患于未然。

2017年中国移动应用安全检测的方法

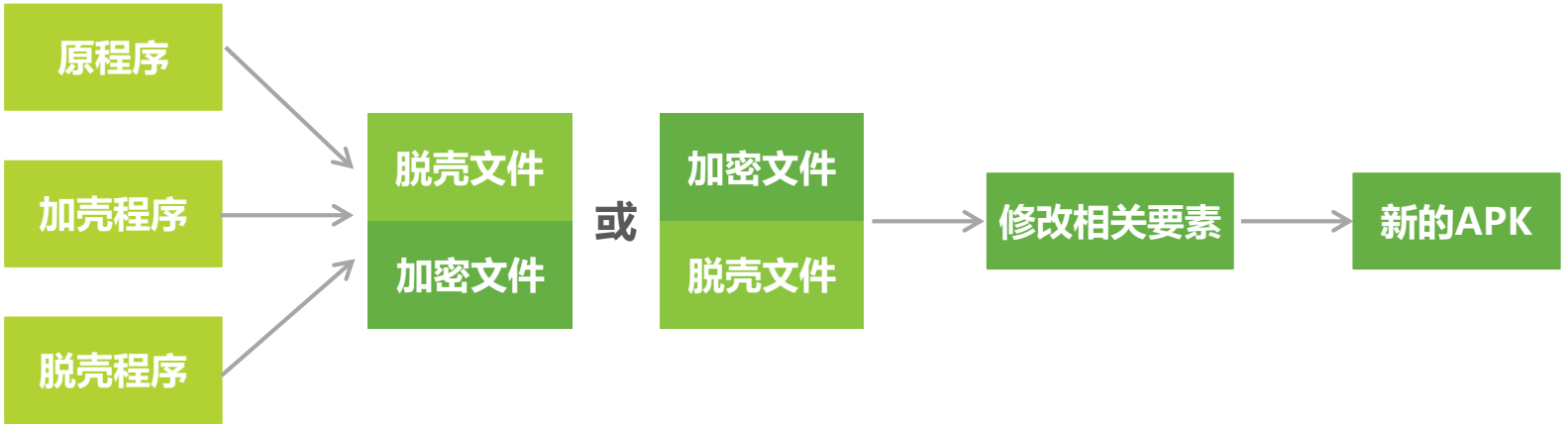
来源：艾瑞研究院自主研究绘制。

安全防护手段-安全加固

将目标程序的入口指向壳程序，阻止攻击者对程序反编译

移动安全加固主要是针对移动应用的dex文件、SO库文件等文件的代码进行的加壳保护，是应用安全的基础。加壳技术的核心目的是帮助应用程序抵御攻击者对其进行反编译，避免核心代码直接暴露在攻击者面前。加壳技术的原理是在原程序中植入一段代码，将目标程序的入口点指向自己的壳，并把原来的程序进行压缩、加密。当程序执行时，首先执行壳程序代码，通过壳程序对原程序进行解密、解压缩和动态加载，此外壳程序还需要对软件的运行环境进行检测，一旦有动态调试，则终止程序运行，从而有效阻止攻击者对程序进行反编译。

2017年中国Android应用软件加壳原理



原程序：需要被保护的程序；　**加壳程序：**对原程序进行加密的代码；
脱壳程序：为加壳后程序进行解密原程序和动态加载原程序的代码。

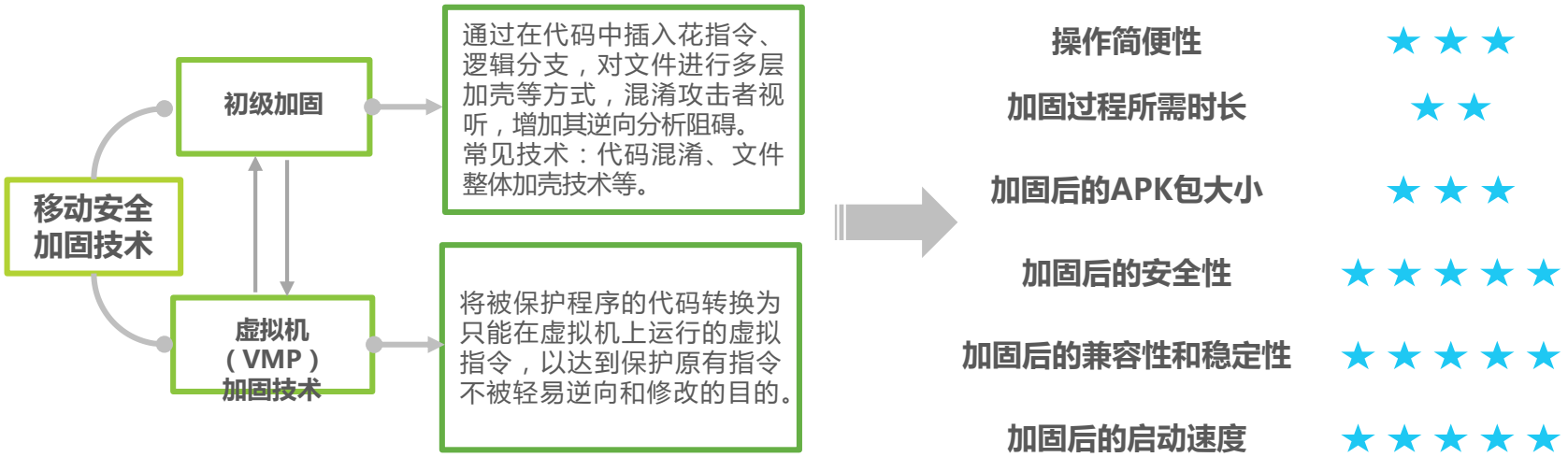
来源：艾瑞研究院自主研究绘制。

安全防护手段-安全加固

VMP技术深度加固，加固后的启动速度和兼容性最为重要

一般而言，针对移动应用程序的加固主要是由初级加固技术和虚拟机（VNP）加固保护技术共同完成的。其中初级加固技术如代码混淆技术、文件整体加壳技术等均是由PC时代的安全保护技术原理引入到移动领域的。他们通过在代码中插入花指令、逻辑分支等方式可以增加攻击者的逆向分析难度，但是本质上原始的程序没有发生变化。而VMP加固技术则是将被保护的可执行代码转换为字节码指令系统的代码，本质上是对原指令系统进行“封装”。
现阶段企业更关注加固后应用的安全性、兼容性、启动速度这三个方面，其中加固后的代码增量也是企业重点考察的方面。

2017年中国常见移动应用安全加固技术及衡量安全加固技术的指标



来源：艾瑞研究院自主研究绘制。

安全防护手段-安全监测

渠道管理、大数据分析、识别仿冒程序是安全监测的核心

移动应用的安全监测的核心在于如何对各应用分发渠道进行管理，以及如何通过海量的数据识别仿冒。因此移动安全监测的核心技术就是渠道管理、识别仿冒程序和大数据分析能力。其中渠道管理保证移动安全企业可以监测到足够的APP数及其详细信息，为他们提供分析和识别的前提；识别仿冒程序是安全监测的核心目标，不仅可以清除潜在威胁，而且可以为开发者反馈仿冒程序的信息，使其针对性地进行策略调整；大数据分析将移动安全企业监测的诸多信息整理并分析，为开发者的开发、管理及推广提供支持。

2017年中国移动应用安全监测的主要技术

渠道管理

主要指对移动互联网的众多应用市场、论坛及其他渠道进行实时有效检测，包括各类APP的版本、下载源、下载量、渠道等。

识别仿冒程序

目前市场仿冒程序的高隐蔽性要求移动安全服务企业需要快速而精准的识别仿冒程序，同时需要将详细信息反馈给开发者，便于开发者对各类仿冒程序的了解。

大数据分析

移动应用分发渠道的多样性和实时变化性要求移动安全服务企业需要建立大数据分析平台，从行业、渠道、版本等多维度分析移动应用安全状况，辅助开发者管理APP在各大渠道的推广运营工作。

来源：艾瑞研究院自主研究绘制。

移动应用安全发展的挑战与机遇

行业的不规范与乱象为移动应用安全企业带来发展新机遇

现阶段随着各种智能终端设备的普及，用户的触网习惯向移动端迁移，因此各类适合移动端的应用不断涌现，整个移动应用市场尤为繁荣。但由于Android平台没有统一的应用下载平台，没有权威的发布机构，更没有统一的监管机构，因此整个移动应用市场生态环境有待整顿。但机遇与挑战并存，移动用户普及率的提升与移动应用下载量的攀升为移动应用安全服务市场带来巨大商机，同时，移动物联网时代的到来将会带动新兴市场的移动安全防护的发展，故在蓝海一篇的移动应用安全市场中将充满各种可能。

2017年中国移动安全行业的挑战与机遇

恶意持续增长：据CNCERT发布的数据显示，2016年的移动互联网恶意程序树立狼为205万余个，较2015年增长39.0%，且近7年来保持持续高速增长趋势；

行业标准缺失：Android市场门槛较低，没有权威发布机构，且审核不严，致使很多移动APP被二次打包后重新投放市场，危害用户隐私及安全；

应用市场缺乏监管：移动应用安全相关法律法规滞后，行业对移动APP安全相关风险认知不足，市场缺乏统一安全标准；

市场供需不对称：目前各行业在移动应用领域的安全是不一样的，市场行业尚未建立通用安全标准，市场供需不统一。

移动用户普及率高：移动互联网发展、智能终端成本降低与普及率提升，用户触达移动端入网门槛持续降低；

移动应用下载量攀升：目前拥有过亿用户的移动应用已达10款左右，包括微信、新浪微博、手机淘宝等，移动APP的下载量随着移动智能设备的普及急剧攀升；

移动应用领域细化与门槛降低：移动应用将不断向更加垂直化、精细化方向深耕，并且随着APP制作的技术门槛的降低，用户定制个性化的APP应用平台，APP市场进一步繁荣；

物联网的发展：自动驾驶、智能家居等物联网的发展，新兴的移动应用安全服务将出现。

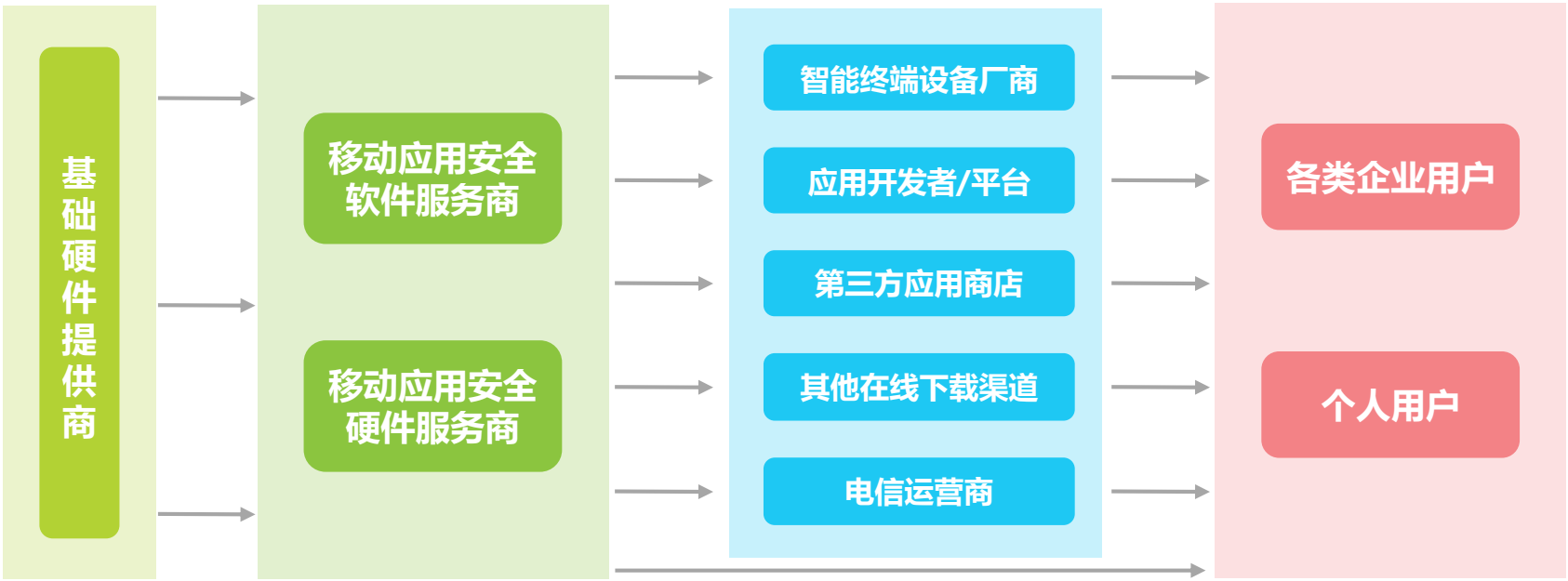
来源：艾瑞研究院自主研究绘制。

移动应用安全服务行业产业链

移动应用安全服务商通过多渠道向多领域提供安全保障服务

在移动应用安全服务行业的整个产业链中，移动应用安全服务商分为软件服务商和硬件服务商，并居于中心位置，其上游为移动智能终端设备厂商，提供基本的硬件设施；下游服务对象主要以企业级用户为主，包含很小一部分的个人用户，二企业级用户则主要为政企、金融、互联网以及物联网等企业，这些企业多覆盖人民生活的方方面面，对安全性要求比较高。而移动应用安全软件服务商既可以直接向用户提供服务，也可以通过应用商店、应用开发者/平台、以及其他的在线下载渠道间接向用户提供服务。

2017年中国移动应用安全服务行业产业链



来源：艾瑞研究院自主研究绘制。

移动应用安全服务市场玩家分布

垂直类和互联网巨头类移动应用安全企业共推行业发展

当前移动应用安全服务市场的玩家主要包含两方，分别为互联网巨头在移动应用安全方面的布局和深耕移动应用安全的垂直创业企业。其中互联网巨头企业通常与自己的业务结合的更加充分，他们的业务广泛，具有较强的使用场景；而垂直类的移动应用安全企业则是随着移动应用安全服务市场的兴起而逐步开始发力参与市场角逐，他们往往面向更多行业，提供更具针对性的解决方案。未来，随着物联网的发展，移动智能设备的应用将更加多元化，将为移动应用安全服务市场带来新的机遇和挑战。

2017年中国移动应用安全行业市场玩家分布

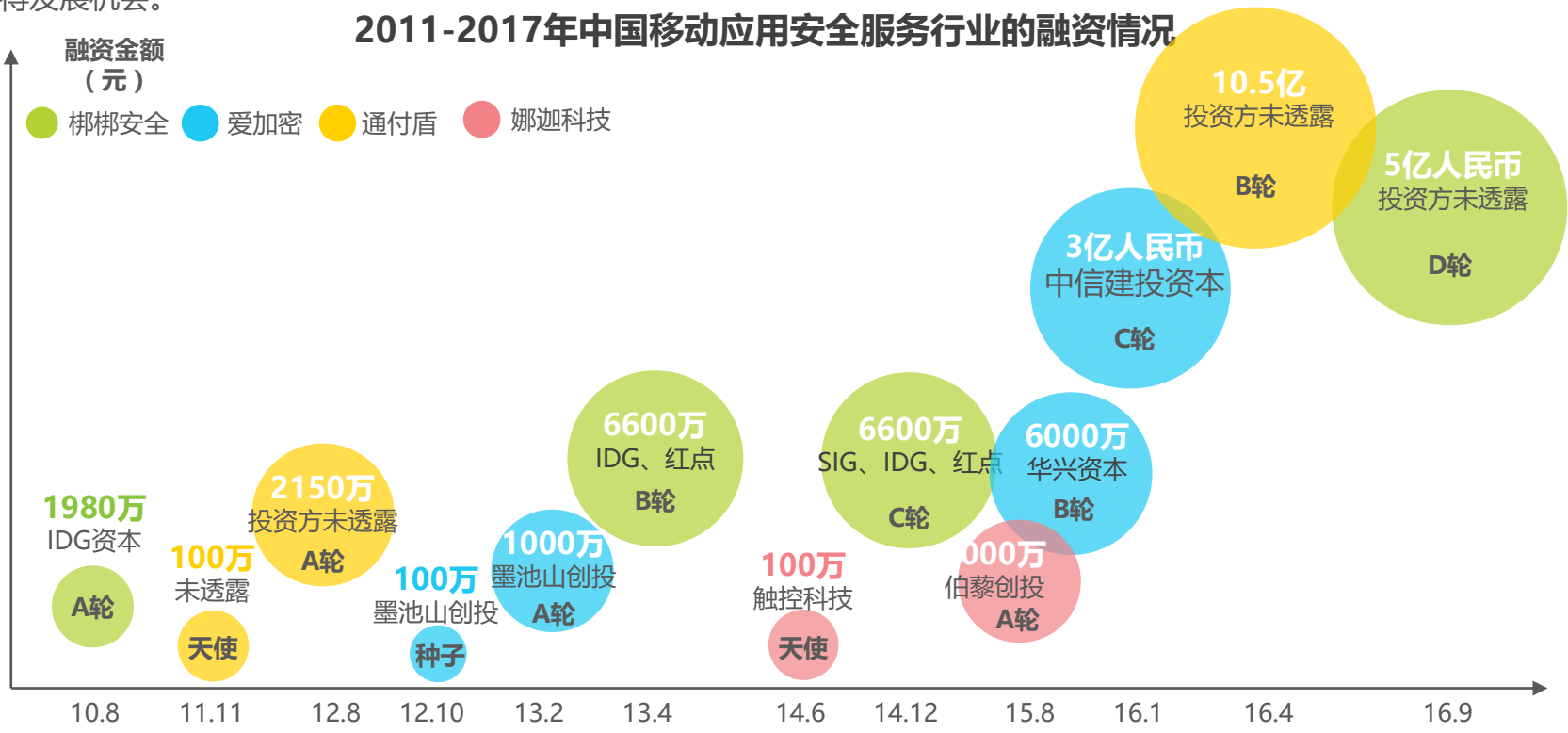
来源：艾瑞研究院自主研究绘制。

移动应用安全行业市场投融资情况

融资规模集中于千万量级，早期融资项目居多

从融资规模来看，企业网盘市场的融资多集中在千万级别。从获得融资的企业数量来看，目前获得融资的市场玩家并不多，资本市场表现的活跃度不高。从融资金额来看，进入B轮及以后的企业获得的融资金额急剧增加，这可能是因为移动应用安全行业的市场开始趋于成熟，并且有较大潜力的发展空间广阔，逐步受到资本的认可。由此可见，移动应用安全服务作为一种以技术驱动为主的高成本的企业级服务，创业型企业的发展需要通过不断融资升级产品及服务，占领市场，从而取得发展机会。

2011-2017年中国移动应用安全服务行业的融资情况



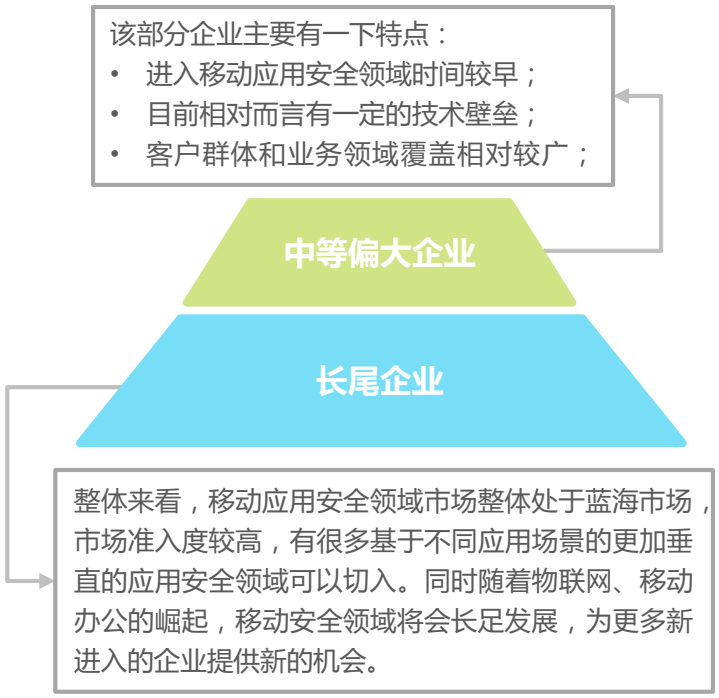
来源：艾瑞咨询研究院自主研究及绘制。

移动应用安全行业市场集中度

市场集中度相对较高，尚未出现龙头企业，市场准入度较高

目前，中国移动应用安全行业处于快速发展的初期阶段，市场集中度相对较高，虽然部分在市场上较为突出的企业进入市场较早，具有一定的技术壁垒，并且业务覆盖相对较广，但市场尚未出现龙头企业，整个市场的准入度较高。从整体市场竞争机会角度而言，针对细分行业的特点和需要保护的内容提供服务、复杂应用的加固保护以及针对恶意应用攻击持续向底层渗透的情况提出新的防护措施等均将提升企业的市场竞争力，建立新的竞争壁垒。

2017年中国移动应用安全服务行业的市场集中度



来源：艾瑞研究院自主研究绘制。

2017年中国移动应用安全服务行业的市场特点

移动应用市场开始细分

移动应用安全服务行业需求正在扩大，不同行业有自己的特点和需要保护的核心内容，因此将在不同行业的定制化保护方案可能会出现。

针对复杂应用的加固保护方案尚需完善

具有复杂应用场景的APP往往采用插件化的思想开发，此时利用通用话的加固方案很难将所有dex文件保护，即dex文件可能会出现无法全部被加密的情况，因此安全服务企业需要有更加全面的加固方案保证核心dex文件被识别并加固。

恶意应用攻击持续向底层渗透，安全风险增加

现阶段，恶意代码在自我保护和加密技术上有了新突破，恶意代码混淆技术进一步发展，并且攻击方式逐步趋于向Linux内核层渗透，对恶意应用程序进行逆向分析的可行性不断降低，因此移动应用所面临的安全问题越来越严峻。

梆梆安全

产品体系全，覆盖业务广，解决方案多样化

梆梆安全成立于2010年，已于2016年9月完成D轮融资，其安全防护产品体系全面，不仅提供APP安全保护、移动威胁情报、事前/事后应急响应等服务，同时面向行业提供全套安全方案，针对业务定向威胁提供贯穿生命周期的纵深防御体系。梆梆安全致力于为政府、企业、开发者和消费者打造安全、稳固、可心的移动应用生态环境，业务遍及金融、互联网、物联网等各大行业。

梆梆安全的主要产品体系、业务布局及对应的解决方案

运营商	对运营商市场、计费SDK、通讯协议、证书及其APP进行安全检测、加固加密服务监控所有APP，实时报告威胁态势；
金融	针对移动应用生命周期（研发、发布、运营）的各个阶段提出不同的安全防护及解决方案；
互联网	针对不同领域的应用特点提出细分的解决方案，以保证应用的完整性、防调试、反编译、资源及数据安全；
政企	梆梆安全企业移动IT套件可以为企业移动弄设备、应用程序和数据，提供一整套安全的防护手段；
IOT	针对智能汽车、智能家电、智能家居等领域提供了应用程序保护、智能云更新及嵌入式固件OTA升级修复漏洞等解决方案；

商业模式

现阶段：向B端提供标准版（免费）和定制版（增值服务）服务，按年收费；
未来：打造安全即服务的模式，届时可按服务种类和装量收费；

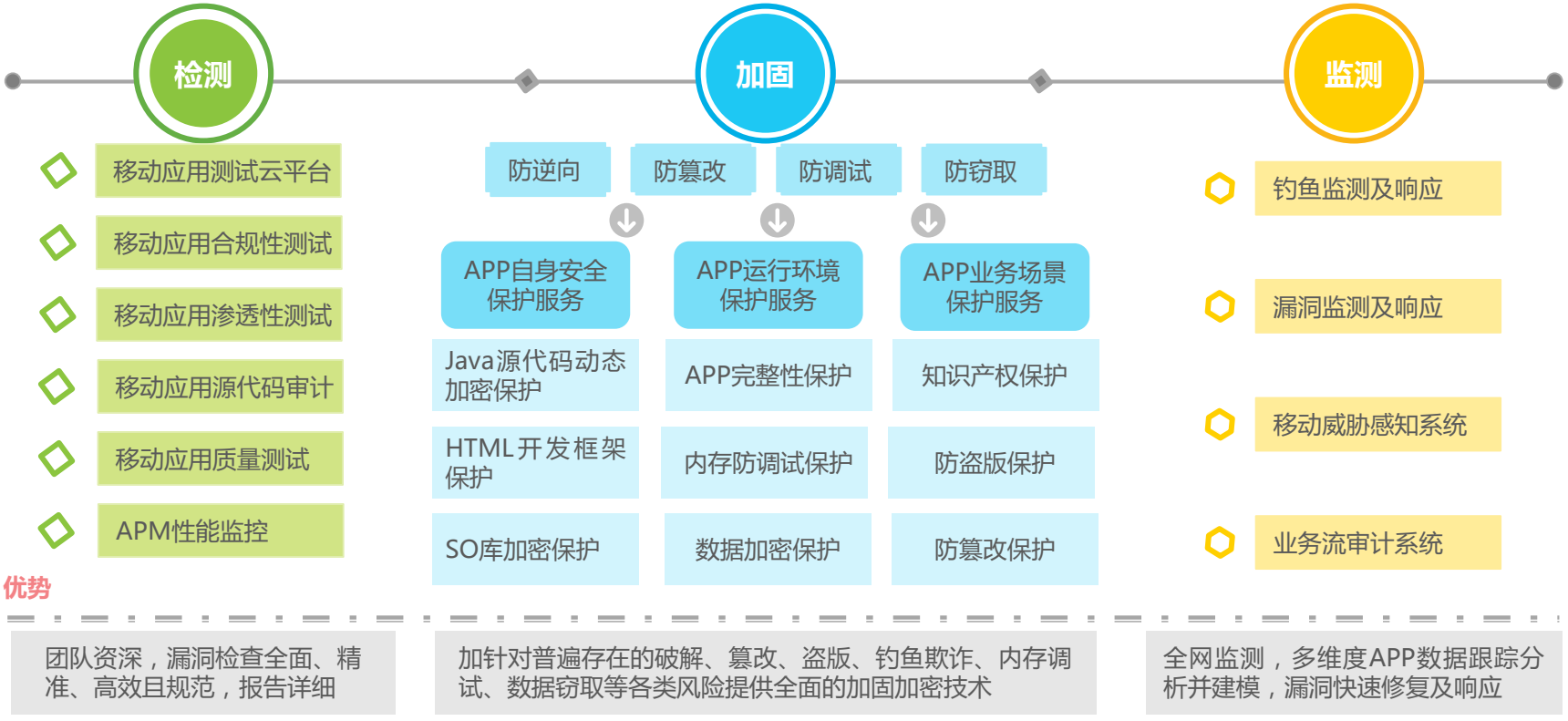
来源：艾瑞研究院自主研究绘制。

梆梆安全

多方位检测及监测、快速安全响应、立体安全防护

梆梆安全的检测功能重点是对应用程序周围环境的坚持，以确定其是否可被信任。检测的主要目的是及时发现各类外部直接或潜伏的攻击；基于威胁情报内容，梆梆安全会通过部署安全服务产品减少被攻击面来提升攻击门槛，并在被攻击前提前拦截攻击动作；通过对全网的监测，将情报进行分析并反馈到防护阶段和检测功能处，可构成整个威胁处理流程的闭环。

梆梆安全的移动应用安全防护技术及其优势



来源：艾瑞研究院自主研究绘制。

通付盾

服务体系全面，业务覆盖广，盈利模式清晰

通付盾成立于2011年，是一家专业的金融科技安全公司，产品线全面覆盖账号风险保护、应用风险保护、欺诈风险保护、信用风险保护四大板块。主要客户覆盖银行、互联网金融、支付行业、电子商务、政府企业等多个领域，主要通过标准化产品及定制服务收费。

通付盾的主要服务体系及业务布局

来源：艾瑞研究院自主研究绘制。

通付盾移动安全

检测+加固+威胁感知+监测四位一体，共保APP应用安全

通付盾APP安全检测与加固严格按照国家标准规范，将自主研发的基于深度学习方法的动静双引擎检测方法运用到安全检测产品中，主动挖掘未知漏洞、发现恶意代码和后门程序，面向Android和iOS提供移动应用程序的全方位安全检测服务；在APP加固方面，通付盾针对移动应用逆向工程、二次打包等攻击行为，将VMP虚拟机保护技术运用到APP加固领域，层层递进，纵深防护；在全渠道应用监测方面，基于对全网APP的监测分析，构建移动应用安全大数据平台。实时监测全网移动应用的漏洞分布、内容违规、盗版仿冒及恶意行为等信息，从行业、渠道、地域等多维度进行分析，呈现全网移动安全态势感知走势，为企业、行业监管部门、渠道市场等提供APP安全全景视图，助力净化移动互联网空间。

通付盾移动应用安全防护技术及其优势

APP安全检测	APP安全加固	APP安全监测	APP威胁感知
• 以符号执行为核心的静态分析引擎； • 以运行沙盒为核心的动态检测引擎； • 深度学习算法；	• 整体加壳保护：防动态调试、内存dump保护、防静态逆向； • 代码混淆：防逆向保护，代码插花、代码膨胀； • VMP保护：核心代码或函数保护，对抗高级恶意攻击；	移动安全态势感知平台实时监测分析移动APP的恶意行为、内容违规等信息，从地域、渠道、行业等多维度挖掘，呈现全网态势感知走势数据和威胁预警数据。	• 环境安全检测：检测设备是否进行root或安装修改器及模拟器，检测终端应用安全，发现、预警并拦截新型恶意应用； • 实时监测各类攻击手段； • 程序实时监测海量终端程序；
• 平台通用性强，全面覆盖Android和iOS系统； • 检测项目全面，包含移动APP客户端和其关联服务器的API接口漏洞检测； • 结果高效精准； • 人工渗透分析专业且经验丰富；	• 高兼容：适配各种机型/系统，兼容Android O/iOS不同系统版本和设备； • 防破解：防篡改、对抗逆向、脱壳工具等效果强； • 低损耗：不涉及功能源码与程序逻辑，不影响程序运行效率；	• 数据全：覆盖全网各应用市场，数百万移动应用； • 多维度：从行业、渠道、地域等多维度分析应用安全状况； • 准实时：实时更新移动应用安全数据； • 精度高：基于动静结合的双引擎分析技术，精准定位风险；	• 设备指纹技术：获取上网设备的软件、硬件、行为等多想属性信息生成全球唯一设备ID; • 全方位立体多维度的大数据存储及分析技术； • 基于深度学习的病毒检测技术：通过对样本不断进行检测训练，更加快速准确定位安全风险；

体验版：提供基础的加固服务，有效期14天；　　**定制版：**在体验版的基础上提供更深层的定制化保护；

来源：艾瑞研究院自主研究绘制。

爱加密

提供基于移动应用、安全大数据等多维度的一站式服务

爱加密成立于2012年，是业内领先的移动应用和物联网安全服务提供商，目前已完成C轮融资。在国家网络安全法等政策的指引下，率先提出了以威胁感知为核心，以安全大数据和业务大数据驱动的移动应用和物联网全生命周期安全解决方案。爱加密以技术为本，是国内多项国家及行业标准制定的参与者，拥有多个权威机构的认证以及软著专利。

爱加密的主要服务体系及业务布局

爱加密 www.ijiami.cn

事前 → 事中 → 事后

服务体系

安全服务
- 安全开发咨询服务
- 安全编码规范咨询服务
- 开发外包安全咨询服务
- 安全规划咨询服务
- 等级保护咨询服务
- 安全风险评估服务等

安全检测
- 源代码审计检测
- 移动应用安全检测
- 安全合规性检测
- 移动应用人工检测

安全加固类型
- Android安全加固服务
- iOS安全加固服务
- H5安全加固服务
- SDK加固服务
- SO库保护
- 短信防劫持平台
- 秘钥白盒
- 服务器防护平台
- 防业务刷单平台
- 环境清场SDK
- 通信协议加密SDK
- 安全软键盘SDK

风险感知
- 移动应用钓鱼及盗版感知响应
- 网络钓鱼监测及响应
- 移动应用威胁感知平台
- 移动应用崩溃感知及响应

业务优化
- 压缩服务
- 推广服务
- 云更新服务
- 多应用融合服务

移动安全治理平台、移动安全大数据、移动威胁态势感知

业务布局

金融 | 政企 | 运营商 | 物联网 | 互联网应用

核心优势

技术优势：双重VMP加固技术、纯净防护无SDK植入；

服务优势：以客户为先遍布全国的专业企业级服务优势；

体系优势：以态势感知为基础，以大数据驱动为核心的智能防御体系；

理念优势：以产品为核心、以技术为导向

方案优势：覆盖移动应用、物联网等完整生命周期解决方案；

权威优势：行业标准的制定者与参与者，拥有完备资质；

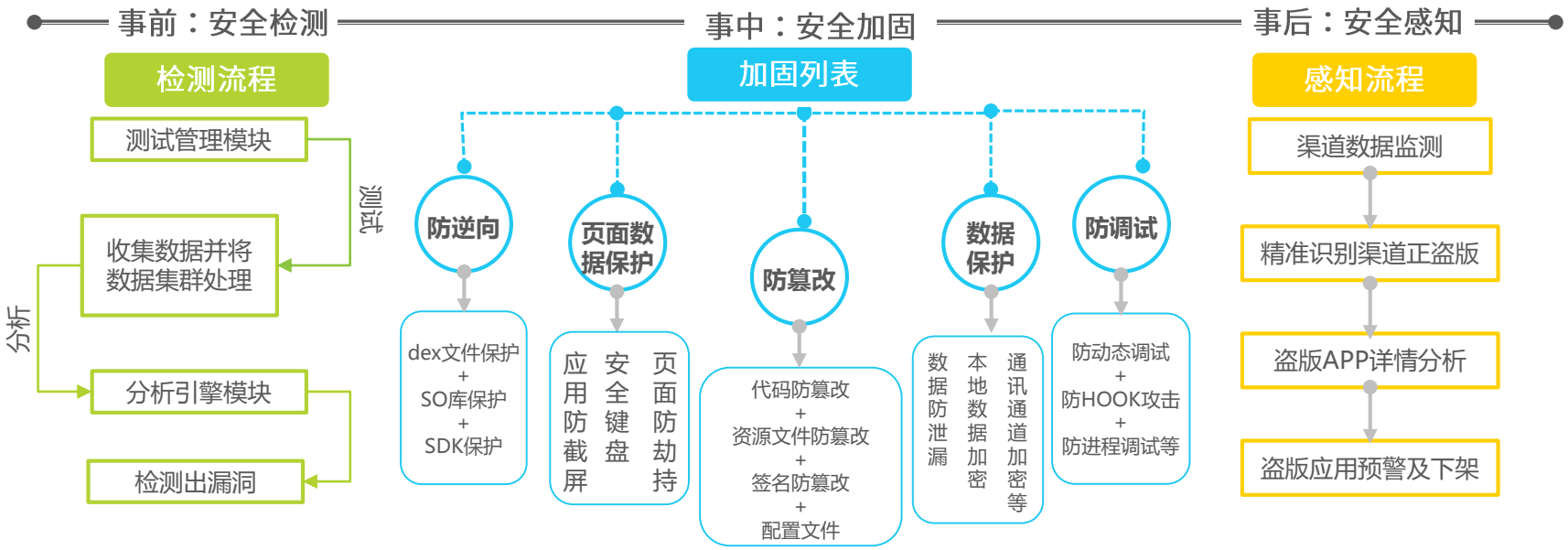
来源：艾瑞研究院自主研究绘制。

爱加密

加固技术先进、破解难度大、加密方式灵活、加固功能全面

爱加密为客户提供了集安全开发、测试、检测、加固、感知及实时盗版监测于一体的综合服务。应用开发阶段提供源码级安全设计和审计方案，开发完成后自动流转到安全测试环节进行性能和兼容性测试。随后根据检测结果自动生成加固策略进行安全加固，加固后再次进行兼容性测试，并与原始应用进行结果对比和差距分析。应用发布后，通过态势感知实时监控安全风险和威胁，盗版监测则能及时发现并预警。感知和监控的结果再次输入到最初的检测、加固环节形成安全防护的闭环。

爱加密的安全防护技术及其优势



优势

技术先进，加固功能强

功能强大，用户体验好

兼容性强，实时兼容最新Android和iOS平台，加固包兼容性高

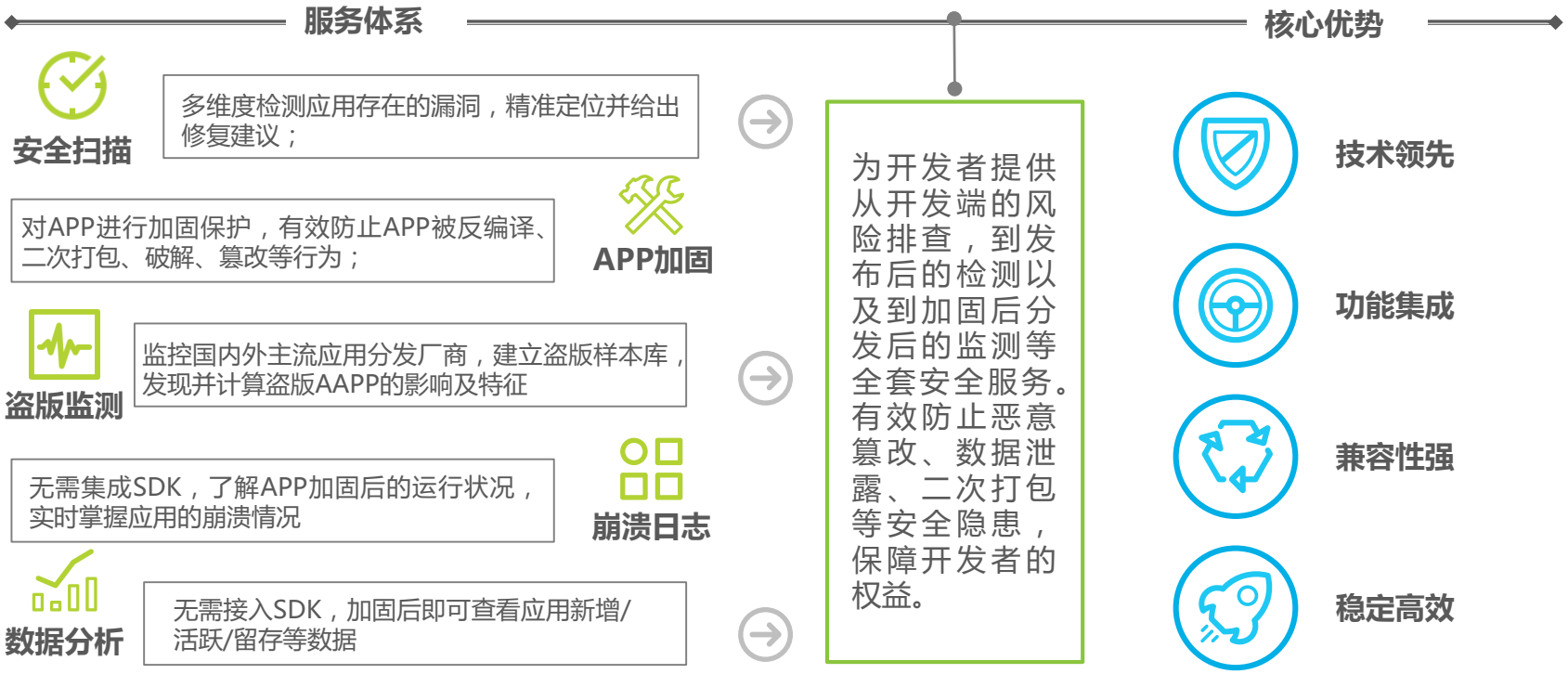
来源：艾瑞研究院自主研究绘制。

360加固保

扫描、加固、监测等服务体系有效保障用户权益，优势明显

360加固保主要是针对APP的整个生命周期提供安全扫描、加固、监测等服务，有效的阻止开发者开发的应用被篡改、二次打包等攻击，从而保障开发者及用户的利益。同时，360加固保还为开发者提供了数据分析、崩溃日志分析等服务，全方位的帮助开发者了解数据健康与运营状况。

360加固保的主要服务体系及其优势



来源：艾瑞研究院自主研究绘制。

360加固保

扫描获悉安全隐患，加固全面且性能好，监测预估影响

360加固保为移动应用开发者提供安全扫描、加固、监测等全套安全防护服务。通过安全扫描可以完成APP上线前的安全评估，发现源代码缺陷及安全功能设计缺陷等安全隐患，帮助开发者提升应用的安全性；360加固服务操作简单，开发者直接上传应用并加固即可，而且加固功能全面，能有有效保护应用不被反编译、恶意篡改、二次打包，保护数据信息不会被窃取。盗版监测不仅可以下载盗版应用，对其进行分析挖掘，并且会将每个盗版应用样本提供给开发者，供其参考，而且能够帮助开发者了解盗版应用的影响范围，以便及时采取措施。

360加固保的移动应用安全防护技术及其优势

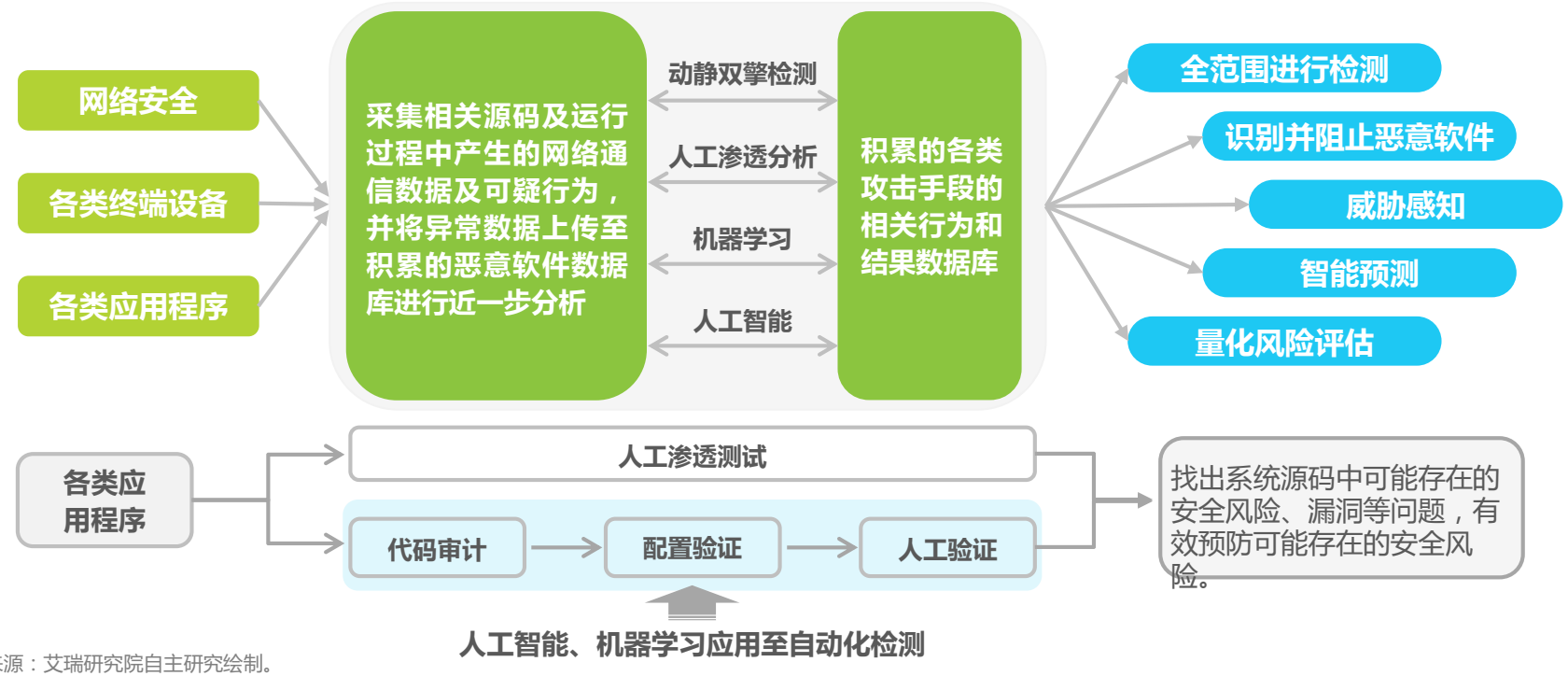
来源：艾瑞研究院自主研究绘制。

人工智能、机器学习提升安全检测质量

人工智能、机器学习逐步成熟，与人工检测共同用于移动应用安全检测，威胁可能被预测及量化，降低安全风险

大数据的积累使得人工智能和机器学习技术可以应用到移动应用安全检过程，相比于传统的人工检测，利用人工智能和机器学习手段不仅可以提升检测效率，降低成本，而且可以更好的分析数据、更有效地检测到安全威胁和漏洞。未来，随着人工智能和机器学习的发展，对应用检测的准确率和效率将会进一步提升，而且其检测的功能性也越来越强，除了准确识别出恶意软件外，对威胁的感知、预测及风险评估能具有前瞻性的功能将在安全防护方面发挥重要作用。

2017年中国人工智能、机器学习将应用至移动应用安全检测



来源：艾瑞研究院自主研究绘制。

移动应用安全生态圈开始形成

企业开始注重将安全服务覆盖至产业链的上下游，打造安全服务的生态闭环

随着攻击软件的不断升级，不断向底层渗透，未来单一的安全服务已经不能满足用户的需求。将安全服务覆盖至整个移动应用产业链的上下游，打造终端设备+电信运营商+安全产商+开发平台+下载渠道+用户的生态闭环，不仅针对应用的整个生命周期提供安全服务，而且有效的保障了各个环节的安全及用户的利益，提升安全服务企业的竞争力，促进行业良性快速发展。

2017年中国移动应用安全生态圈开始形成

来源：艾瑞研究院自主研究绘制。

公司介绍/法律声明

公司介绍

艾瑞咨询成立于2002年，以生活梦想、科技承载为理念，通过提供产业研究，助推中国互联网新经济的发展。在数据和产业洞察的基础上，艾瑞咨询的研究业务拓展至大数据研究、企业咨询、投资研究、新零售研究等方向，并致力于通过研究咨询的手段帮助企业认知市场，智能决策。

艾瑞咨询累计发布数千份新兴行业研究报告，研究领域涵盖互联网、电子商务、网络营销、金融服务、教育医疗、泛娱乐等新兴领域。艾瑞咨询已经为上千家企业提供定制化的研究咨询服务，成为中国互联网企业IPO首选的第三方研究机构。

版权声明

免责条款

本报告中行业数据及相关市场预测主要为公司研究员采用桌面研究、行业访谈、市场调查及其他研究方法，并且结合艾瑞监测产品数据，通过艾瑞统计预测模型估算获得；企业数据主要为访谈获得，仅供参考。本报告中发布的调研数据采用样本调研方法，其数据结果受到样本的影响。由于调研方法及样本的限制，调查资料收集范围的限制，该数据仅代表调研时间和人群的基本状况，仅服务于当前的调研目的，为市场和客户提供基本参考。受研究方法和数据获取资源的限制，本报告只提供给用户作为市场参考资料，本公司对该报告的数据和观点不承担法律责任。

联系我们

咨询热线 400 026 2099
联系邮箱 ask@iresearch.com.cn
集团网站 http://www.iresearch.com.cn

艾瑞咨询官方微信

生活梦想 科技承载

TECH DRIVES BIGGER DREAMS

iResearch

艾 瑞 咨 询