物联网安全事件频发，市场规模进入快速增长期

2019.3.25

温朝会(分析师)
电话：020-88836105
邮箱：wenchh@gzgzhs.com.cn
执业编号：A1310516100001

摘要：

【物联网安全事件频发，市场规模复合增长率达到 33.2%】

我国物联网安全事件 2018 年前三季度比 2017 年增长高达 138%，物联网系统所会遇到的安全问题总体可以归纳为两个方向数据被泄露和网络瘫痪。目前物联网的安全体系主要是解决感知层的安全，从物联网安全网关、物联网扫描器以及物理网态势感知平台三部分入手，实现感知设备层面的安全防护，防入侵、防扫描、防漏洞、配置检查以及资产和威胁。根据 MarketsandMarkets 预测，2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，即 **2015 年至 2020 年的复合年增长率（CAGR）为 33.2%。**

【“智慧+产业”面临新一轮安全大考】

智慧城市：大量涉及国家安全、经济发展、社会公共利益和个人的重要数据一旦泄露，将对城市的运行和管理造成重大打击并难以恢复，导致城市日常生活瘫痪或造成重大经济损失，目前主流有十个建设智慧城市的要点。**智慧安防**：2017 年中国门禁系统市场规模近 170 亿元，据预测 2018 年中国门禁系统市场规模有望突破 200 亿元。防御安全主要从数据源、安防领域网规范安防领域的安全构建。**智慧环保**：智能环境的安全风险是攻击智能阀门，导致废水溢出；劫持系统设备；操纵命令并且阻碍系统响应；利用传感器跟踪活动。由于主要是攻击设备应用层，目前主流的应对方式是实时监控，注意异常事项的出现。**智慧政务**：政务系统安全主要面临着 ISV 安全开发能力不足、缺乏纵深防御体系、缺乏未知威胁监测能力以及缺乏整体持续监控能力，因此应对的方法是增强主机安全防御能力、Web 安全防御能力、DDoS 攻击防御能力以及整体态势感知能力等。

【物联网设备端潜在的发展契机】

芯片：2017 年我国安全芯片市场接近 80 亿元，芯片级的网络安全必须以 EDA 工具为核心，首先是芯片层面的跨频道攻击防护策略，其次是供应链的安全管理机制，第三则是芯片内部逻辑单元的木马侦测能力。**摄像头**：存在的漏洞类型包括命令注入、授权、信息泄露、缓冲区溢出、弱口令、文件操作、XSS、拒绝服务、目录遍历、固件漏洞等。从根本上解决摄像头安全问题，需以安全管理和安全技术相结合。**云平台**：出现的安全威胁主要在数据存储、访问以及传输过程中。数据传输的安全主要通过加密进行，实现加密储存，依赖于安全存储系统，安全存储系统包括四个部分：存储阵列、PCI 加密卡、安全管理中心、密管代理。

【投资逻辑及重点标的】

物联网安全市场处于快速增长期，“智慧+产业”以及物联网设备安全防护存在广泛的市场空间，建议重点关注全面布局物联网安全的卫士通以及在商用密码应用和数据安全防护方面具有竞争优势的中宇万通和优炫软件。

【风险提示】物联网市场发展不及预期的风险，目前我国网络安全方面的投入占整个 IT 比重仅约 2%，远低于欧美国家 10%左右的水平，预计恶性安全事件将刺激物联网安全市场发展。

相关报告

1、【行业深度】万物互联时代开启，智能控制器迎来黄金期—20171027

2、【物联网专题】率先受益万物互联，无线模组行业进入快车道—20180705

3、小米 IOT 业务成为增长新引擎，重点关注小米产业链投资机会—20180830

4、小米 AIoT 开发者大会召开，联合业界伙伴打造消费物联网龙头—20181129

目录

图表目录

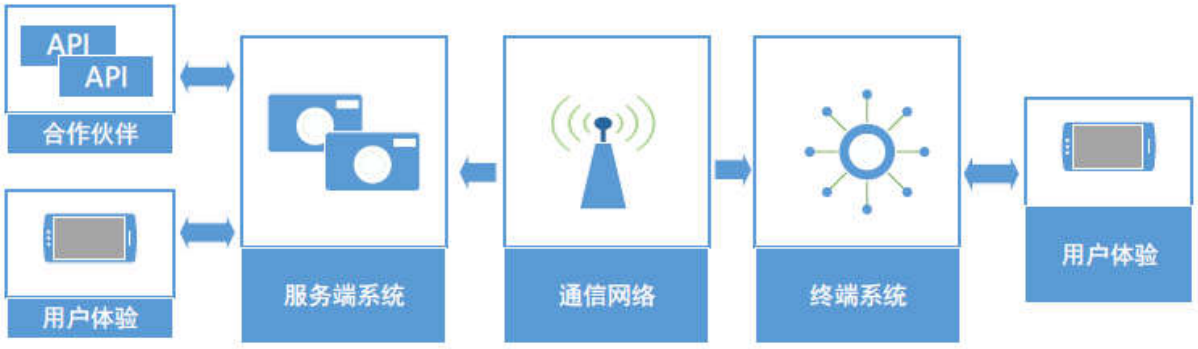
1、物联网安全事件频发，安全市场成新的关注点

1.1 物联网设备直接暴露在互联网极易引致安全问题

物联网将每一个可以单独行使功能的物体用电子标签联结，从而实现万物联通。人们可以通过物联网对机器、设备和人员进行集中管理、搜寻位置，实现物与物之间的信息交换与共享。

物联网的模型主要包括服务端系统、终端系统和通信网络，最具有物联网特色的是终端系统(由各种各样的传感器、协议转换网关、通信网关、智能终端、刷卡机、智能卡等终端设备组成)；通过运行、管理和控制终端系统从而实现物联网系统的操作。

图表 1 物联网应用系统模型

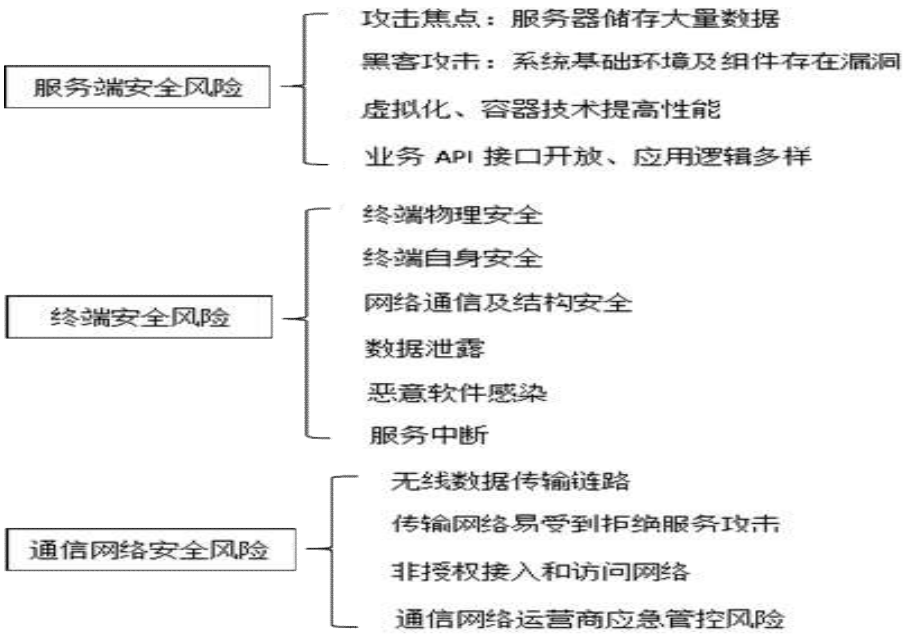


资料来源：物联网安全白皮书 2018、广证恒生

由于大量的物联网设备直接在互联网中暴露，一旦设备存在的漏洞被利用，容易导致设备被控、用户隐私泄露、云服务端数据被窃取以及基础通信网络遭破坏等的安全风险。

一般物联网攻击分为四个步骤，分别是：静态分析、扫描、情报收集、发起攻击。物联网系统所会遇到的安全问题按照其应用系统的模型可以分为服务端、终端和通信网络的风险，总体可以归纳为两个方向数据被泄露和网络瘫痪。

图表 2 物联网安全风险类型

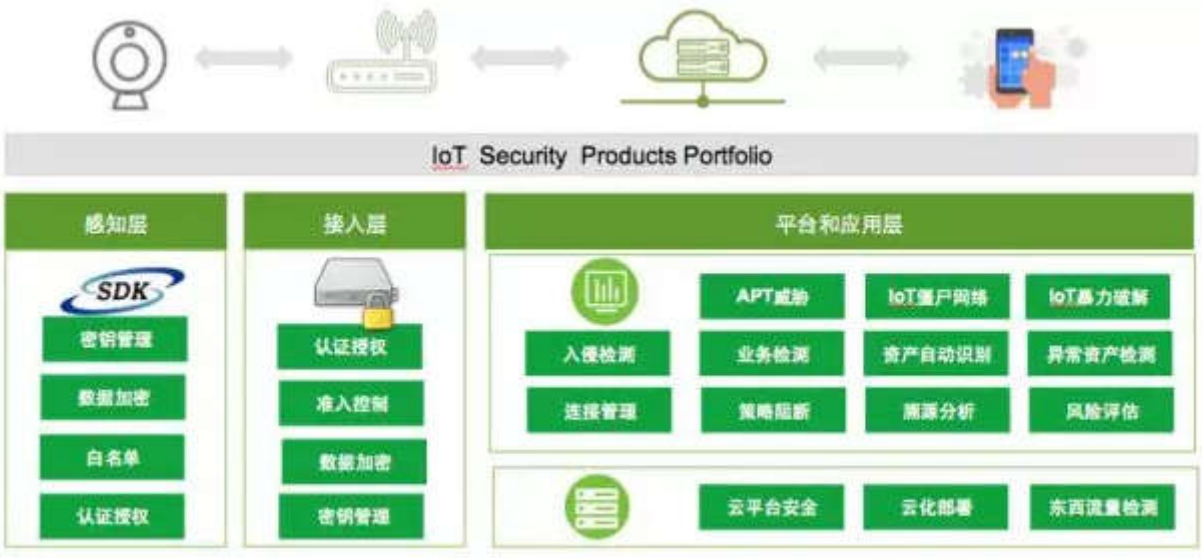


资料来源：物联网安全白皮书 2018、广证恒生

综上所述，物联网攻击主要通过硬件、软件和网络这三个方面进行，而目前我们所需要防范的物联网安全威胁主要来源了数据隐私的泄露和网络系统的攻击导致的瘫痪这两个方面。

目前物联网的安全体系主要是解决感知层的安全，从物联网安全网关、物联网扫描器以及物理网态势感知平台三部分入手，实现感知设备层面的安全防护，防入侵、防扫描、防漏洞、配置检查以及资产和威胁。

图表 3 物联网安全体系



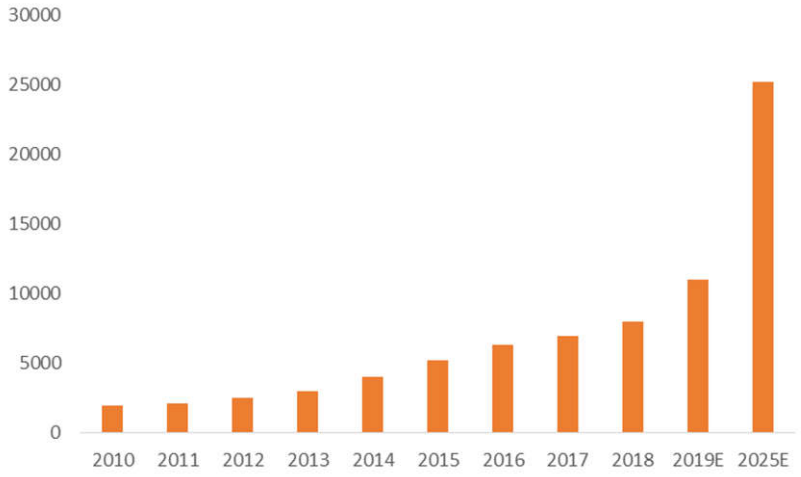
资料来源：绿盟科技、广证恒生

1.2 资金+市场+政策三驾马车，物联网安全备受瞩目

1.2.1 物联网安全支出激增，未来市场空间可期

近几年全球物联网产业发展迅猛，规模急速壮大，根据 IDC 数据，2018 年，全球物联网连接数（包括蜂窝及非蜂窝）达到 115 亿，预测 2020 年将接近 300 亿。同时我国已将物联网列为国家重点发展的战略性新兴产业。预计到 2022 年物联网市场规模将达到 7.2 万亿元。

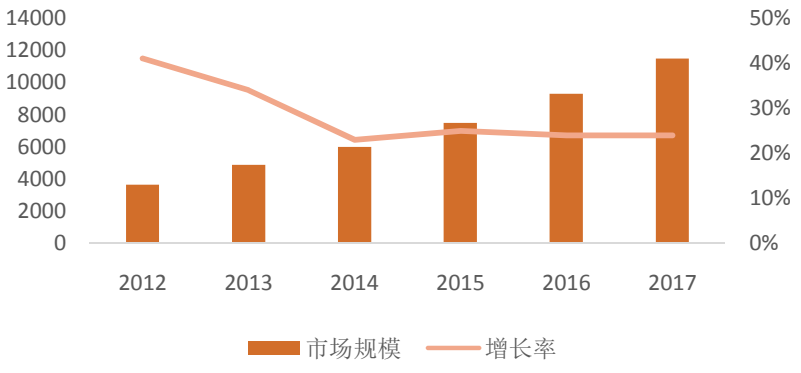
图表 4 2010-2025E 年全球物联网设备网数量（百万）



资料来源：物联网安全白皮书 2018、广证恒生

再者，我国物联网市场空间巨大，根据中商产业研究院的数据，物联网从 2012 年开始发展稳步增长，到 2016 年年复合增长率为 25.8%；2017 年中国物联网市场规模达到 11500 亿元，增长率为 24.0%。我国物联网还未达天花板，用户数逐年提升，2017 年新增物联网用户 1.45 亿元，根据工信部数据显示，截至 2018 年 6 月底，全国物联网终端用户已达 4.65 亿元。与物联网终端设备量的数据相比，用户数量只占不到十分之一，未来物联网市场上涨空间可观。

图表 5 2012-2017 年中国物联网市场规模（亿元）及增长率（%）



资料来源：中商产业研究院、广证恒生

然而伴随着物联网产业的高速发展，物联网攻击事件频发:隐私泄露、非法入侵、局部网络破坏等。未来随着物联网规模进一步扩大，攻击物联网的破坏力将进一步扩大，其安全问题越来越成为社会的关注点。

我国物联网安全事件 2018 年前三季度比 2017 年增长高达 138%，预计 2019 年我国物联网的事发数量将从 2018 年的 7648 件增长至 56121 件，与 2018 年相比增长近六倍。

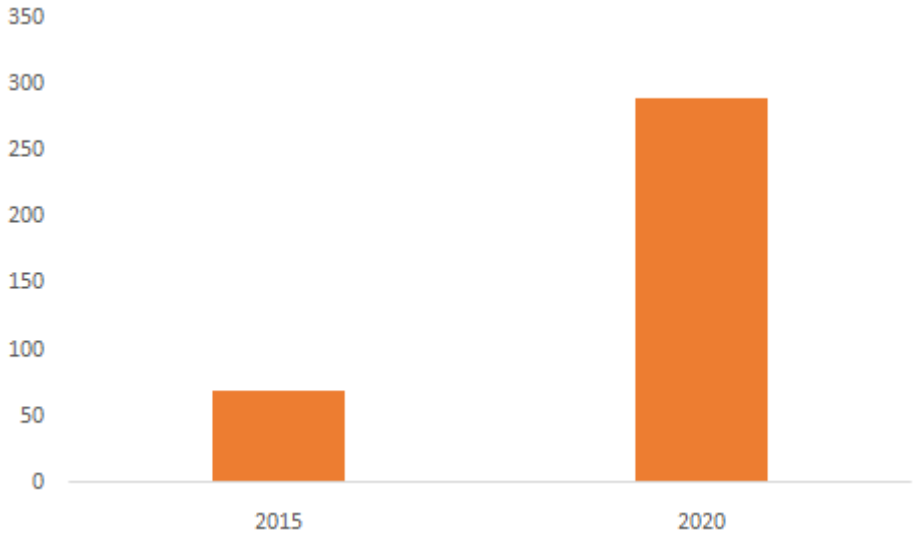
图表 6 2013-2018 年全球物联网发生的安全事件

时间	事件
2018 年	媒体曝出全球最大 CPU 制造商、迎来知天命之年的英特尔遭遇“史诗级”漏洞的冲击。有意思的是，这个问题其实覆盖了主要 CPU 生厂商，并非英特尔一家，影响全球所有桌面系统、电脑、智能手机及云计算服务器。
2018 年	国家药监局发布大批医疗器械企业主动召回公告，其中美敦力、GE、雅培等大牌均在列。召回设备包括磁共振成像系统、麻醉剂、麻醉系统、人工心肺机等。公告显示召回共涉及设备产品超过 24 万，主要原因在于软件安全性不足。
2017 年	成都双流连续发生多起无人机(无人飞行器)黑飞事件，导致百余架次航班被迫备降或返航，超过万名旅客受阻滞留机场，经济损失以千万元计，旅客的生命安全和损失更是遭到了巨大的威胁。
2017 年	美国自动售货机供应商 Avanti Markets 遭遇黑客入侵内网。攻击者在终端支付设备中植入恶意软件，并窃取了用户信用卡账户以及生物特征识别数据等个人信息。该公司的售货机大多分布在各大休息室，售卖饮料、零食等副食品，顾客可以用信用卡支付、指纹扫描支付或现金支付的方式买单。Avanti Markets 的用户多达 160 万。
2016 年	美国最主要的 DNS 服务商 Dyn 遭遇大规模 DDoS 攻击，导致 Twitter、Netflix、Spotify、AirBnb、CNN、华尔街日报等数百家网站无法访问。此次网络攻击中，黑客利用了大量的物联网设备，影响之恶劣可谓是“史上最严重 DDoS 攻击”。
2015 年	HackPWN 安全专家演示了利用比亚迪云服务漏洞，开启比亚迪汽车的车门、发动汽车、开启后备箱等操作。
2014 年	360 安全研究人员发现了特斯拉 Tesla Model S 车型汽车应用程序存在设计漏洞，该漏洞可致使攻击者可远程控制车辆，包括执行车辆开锁、鸣笛、闪灯以及车辆行驶中开启天窗等操作。
2013 年	美国知名黑客萨米·卡姆卡尔在“优兔”网站发布一段视频，展示他如何用一项名为 SkyJack 的技术，使一架基本款民用无人机能够定位并控制飞在附近的其他无人机，组成一个由一部智能手机操控的“僵尸无人机战队”。

资料来源：DoNews、360 企业安全网、新浪新闻、国家药监局、广证恒生

根据物联网安全白皮书，在过去 3 年内接近 20%的企业或相关机构至少遭受一次物联网的攻击，因此企业不断加大在物联网安全防卫方面的支出，根据 MarketsandMarkets 预测，2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，即 2015 年至 2020 年的复合年增长率(CAGR)为 33.2%。安全支出的增加侧面反映了物联网安全防护的需求在日益增加，未来物联网安全领域将会是物联网发展的重要方向。

图表 72015-2020 年全球物联网安全支出预测（亿美元）

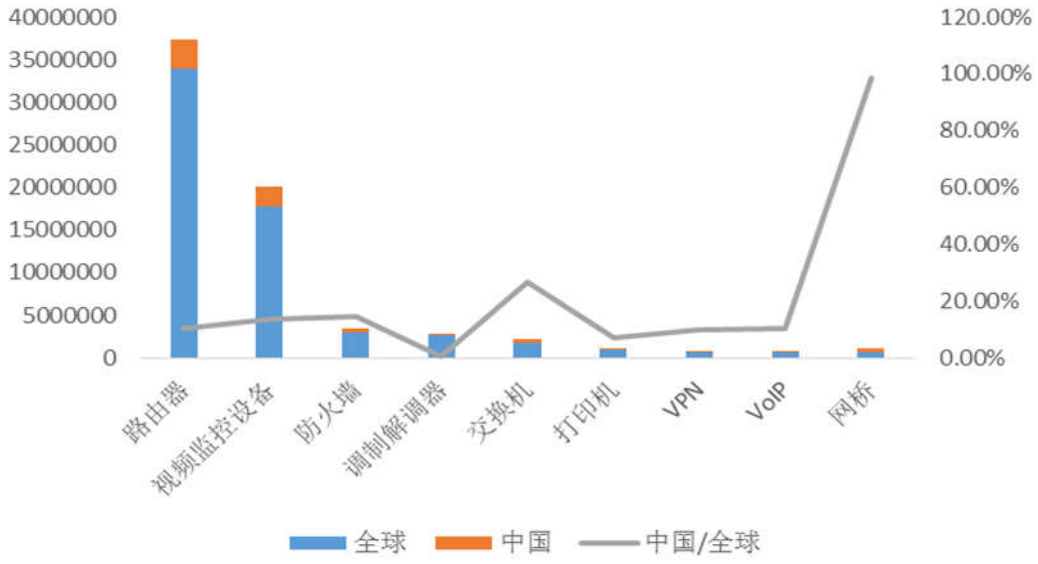


资料来源：MarketsandMarkets、广证恒生

1.2.2 我国物联网设备暴露于互联网数量居全球前列，安全风险系数高

物联网容易出现安全问题主要是由于设备暴露于互联网，容易被黑客等不法份子所利用。而我国的物联网设备暴露于互联网的设备占全球总的 12.42%，路由器、视频监控设备等各类设备暴露于互联网与全球的比例基本超过 10%以上，其中网桥占比高达 98.46%。我国物联网设备暴露于互联网的数量位居全球前列，面临较高的安全风险威胁，因而物联网安全是未来我国在发展物联网的道路上首先面临的一大难题，也是必须攻陷的一座大山。

图表 8 中国与全球设备暴露于互联网的情况



资料来源：物联网安全白皮书 2018、广证恒生

1.2.3 政策支持，物联网安全市场有望进一步加大投入

产业的发展离不开国家政策的支持，从 2013 年国家开始提出物联网专项发展战略到今天，物联网产业跟随着政府制定的产业发展的战略部署，一步一个脚印发展到今天，基本框架已经构建起来，物联网已经被列为国家重点发展的战略性新兴产业。在 2018 年工信部紧跟着出台了《物联网安全白皮书》，将目前物联网安全的现状、防护策略发展方向一一详细阐述，可见国家目前十分重视物联网安全问题尽快的落地。

同时在今年刚刚召开的两会上，人大代表郭永宏建议完善监管体系保护用户隐私，可见现在各界人士都在关注物联网安全的问题，如何做好物联网的防护工作是下一个阶段的重心，政府重视这个问题有望投入更多的财政支持物联网安全工作的开展。

图表 92013-2018 年物联网相关的政策文件梳理

时间	文件	部门	内容
2018 年	《物联网安全白皮书》	工信部	详细分析了物联网安全发展的态势、风险模型、防护策略以及未来发展展望
2017 年	《物联网“十三五”规划》	工信部	明确了物联网产业“十三五”的发展目标：完善技术创新体系，构建完善标准体系，推动物联网规模应用，完善公共服务体系，提升安全保障能力等具体任务。
2016 年	《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》	十八届五中全会	“十三五”规划将全面落地，助力物联网行业加速发展。物联网智能化已经不再局限于小型设备阶段，而是进入到完整的智能工业化领域。
2015 年	《车联网发展创新行动计划》（2015-2020）	工信部	推动车联网技术研发和标准制定，组织开展车联网试点，基于 5G 技术的车联网示范。
2013 年	《物联网发展专项行动计划(2013-2015)》	发改委	包含了顶层设计、标准制定、技术研发、应用推广、产业支撑、商业模式、安全保障、政府扶持、法律法规、人才培养 10 个专项行动计划。各个专项计划从各自角度，对 2015 年物联网行业将要达到的总体目标作出了规定。

资料来源：政府文件、物联网安全白皮书 2018、广证恒生

2017 年我国出台了国家网络安全等级保护基本要求，包括云安全等级保护，移动互联网的等级保护，工业互联网的等级保护和物联网等级保护，而在 2018 年 12 月 28 日，全国信息安全标准化技术委员会的 27 项国家标准正式发布，其中涉及到物联网安全的就有 5 个标准将于 2019 年 7 月 1 日正式施行。

图表 105 个物联网安全方面的国家标准梳理

编号	文件名	内容
GB/T 37044-2018	《信息安全技术物联网安全参考模型及通用要求》	统领性安全标准。本标准规定了物联网安全参考模型，包括物联网安全对象、物联网安全架构和物联网安全措施，并针对物联网系统提出了安全通用要求。
GB/T 36951-2018	《信息安全技术物联网感知终端应用安全技术要求》	对物联网感知终端安全的技术要求。有基础级和增强级两档。对感知终端的物理、系统、接入、通信和数据做了要求。
GB/T 37024-2018	《信息安全技术物联网感知层网关安全技术要求》	对物联网感知层网关安全技术要求。从安全环境，设备安全，访问控制，入侵检测，安全审计以及安全保障做了要求。
GB/T 37093-2018	《信息安全技术物联网感知层接入通信网的安全要求》	接入是指连接感知终端和信息网络构成物联网应用的中间通路和环节，对接入安全要求。有基本级和增强级两档。感知设备标识，接入认证，访问控制、入侵防护，隔离防护，密钥管理，日志等技术要求
GB/T 37025-2018	《信息安全技术物联网数据传输安全技术要求》	对物联网传输的一般数据和敏感数据的安全技术要求。有基础级（一般数据）和增强级（敏感数据）两档。

资料来源：信息安全标准化技术委员会、广证恒生

1.3 物联网安全主题下，建议关注“智慧+”和设备领域

从物联网系统体系来看，投资方向可以从感知层、网络层、平台层和应用层这四个部分。感知层主要是采集信息识别物体，这里容易出现信息泄露，识别有误的安全问题，相关投资方向为芯片和摄像头；而网络层主要是传递和处理感知层信息，涉及的投资方向主要是传感器；平台层主要是各类应用推动成果转化，主体是软件和 APP；最后的应用层主要是垂直领域，将物联网与用户相结合起来为智能终端，涉及智慧+产业主题、车联网和工控安全这几个方面。

图表 11 物联网体系架构

资料来源：公开资料、广证恒生

车联网和工控安全主要涉及自动控制系统，通过破坏自带控制系统从而危害安全。工控系统向工控物联网升级，有效地提高了工作效率，降低了工作成本。目前我国的工控系统还在发展的过程中未来这块的市场空间可期。

而车联网方面，主要是依托智能汽车，而据 GSMA、SBD 预测，到 2018 年，全球车联网市场规模将达到 400 亿欧元，渗透率将达到 20%。车联网安全领域也有可观的市场空间。

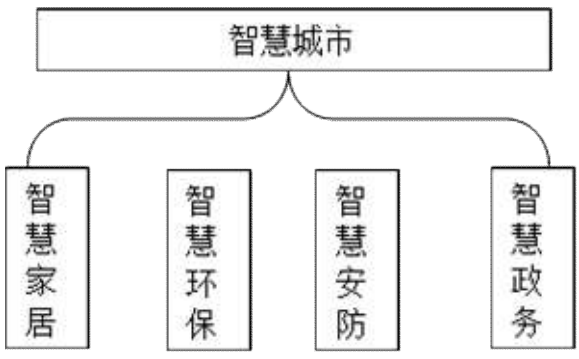
图表 12 物联网安全相关的投资方向

资料来源：公开资料整理、广证恒生

除了车联网和工控安全之外，还有”智慧+产业”市场值得重点关注。今年总理在政府工作报告中指出，打造工业互联网平台，拓展“智能+”，为制造业转型升级赋能。”智慧+产业”这几年已经小有发展，进一步的发展空间更多体现在如何更安全、更高效的实现。

智能城市不仅仅是一个物联网解决方案，它可以看成是一个总体解决方案，捆绑了各种元素，如智慧生态、智慧安防、智慧政务、智慧环保、智慧停车、智慧医疗等等。

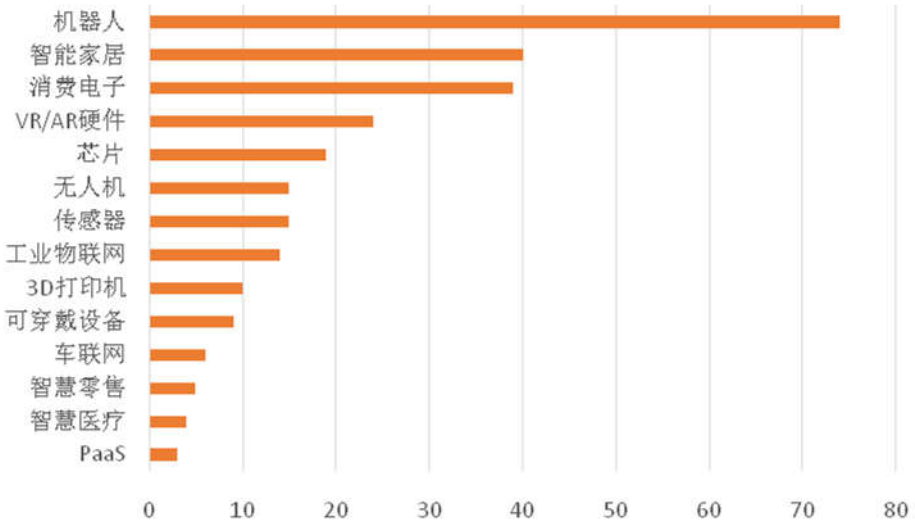
图表 13“智慧+产业”投资方向



资料来源：公开资料整理、广证恒生

从 2017 年物联网的投资数据来看：我国物联网投资交易数为 363 笔，全球物联网投资交易数为 895 笔，可见在物联网方向中国占全球投资总量高达 40.56%，投资人一致看好物联网的发展前景。再从投资的细分领域来看，应用层更多投资于机器人、智能家居、消费电子；设施方面 VR/AR 硬件、芯片和传感器是投资人关注的重点。因而后面的细分领域重点剖析应用层“智慧+”和设施方面的芯片等投资者较为关注的领域。

图表 142017 年我国物联网细分领域投资笔数



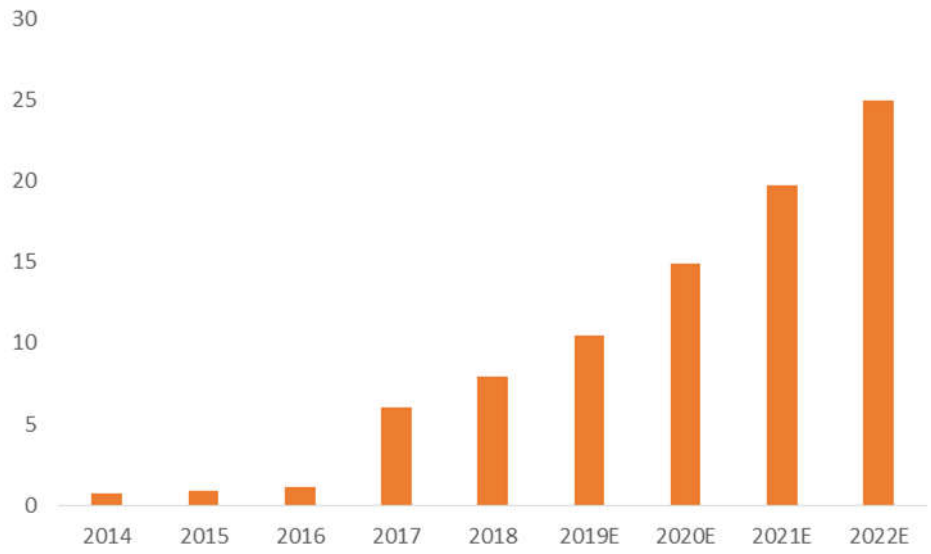
资料来源：《2017-2018 中国物联网发展年度报告》、广证恒生

2、“智慧+产业”面临新一轮安全大考

2.1 智慧城市：构建核心安全体系层层击破

智慧城市建设已经成为全球热点，当前全球已启动或在建的智慧城市数量超过 1000 个，中国以 500 个试点城市居于首位，成为了全球最大的智慧城市实施国。据 IDC 分析估计，2018 年中国智慧城市相关投资将突破 200 亿美元，并在 2016-2021 年保持近 20%的复合增长率。到 2021 年，中国智慧城市市场规模将有望达到 350 亿美元。

图表 152014-2022E 年中国智慧城市的市场规模（万亿元）

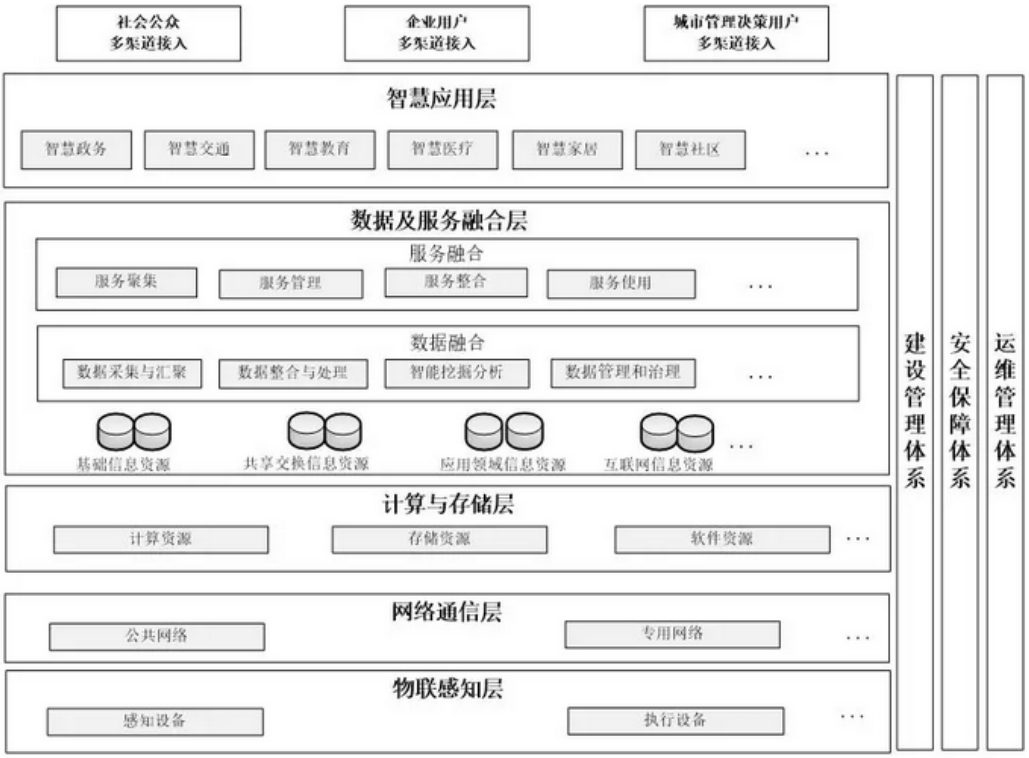


资料来源：前瞻产业研究院、广证恒生

基于国内通用的智慧城市建设的主流模型，五个层次都可能面临着各类不同的安全威胁:**物联感知层**的感知设备被攻击篡改、执行设备被攻击篡改、利用伪基站对移动终端的攻击、劫持终端感知设备发动 DDoS 攻击等威胁；在**网络通讯层**可能会遇到物理攻击、网关节点捕获、普通节点捕获、传输截获、传输窃听、传输篡改、传输伪造、DDoS 攻击、重放攻击、完整性攻击、黑洞攻击、虫洞攻击等一系列传统与新兴网络攻击及其变种；**在计算与存储层**物理破坏攻击、物理灾难风险、存储和安防架构风险、敏感数据泄露、拖库、撞库、恶意数据注入等威胁；**在数据及服务支撑层**，大数据成为网络攻击的显著目标、大数据加大隐私泄露风险；**在智慧应用层**，网站内容被篡改、0day 漏洞、钓鱼网站、僵尸网络攻击、木马攻击、蠕虫攻击、病毒攻击；

智慧城市中存在着安全隐患：大量涉及国家安全、经济发展、社会公共利益和个人的重要数据一旦泄露，将对城市的运行和管理造成重大打击并难以恢复，导致城市日常生活瘫痪或造成重大经济损失，所以安全保障作为智慧城市可持续发展的根基。随着智慧城市广大的市场空间，智慧城市安全的市场空间可观。

图表 16 智慧城市 ICT 视角的技术参考模型

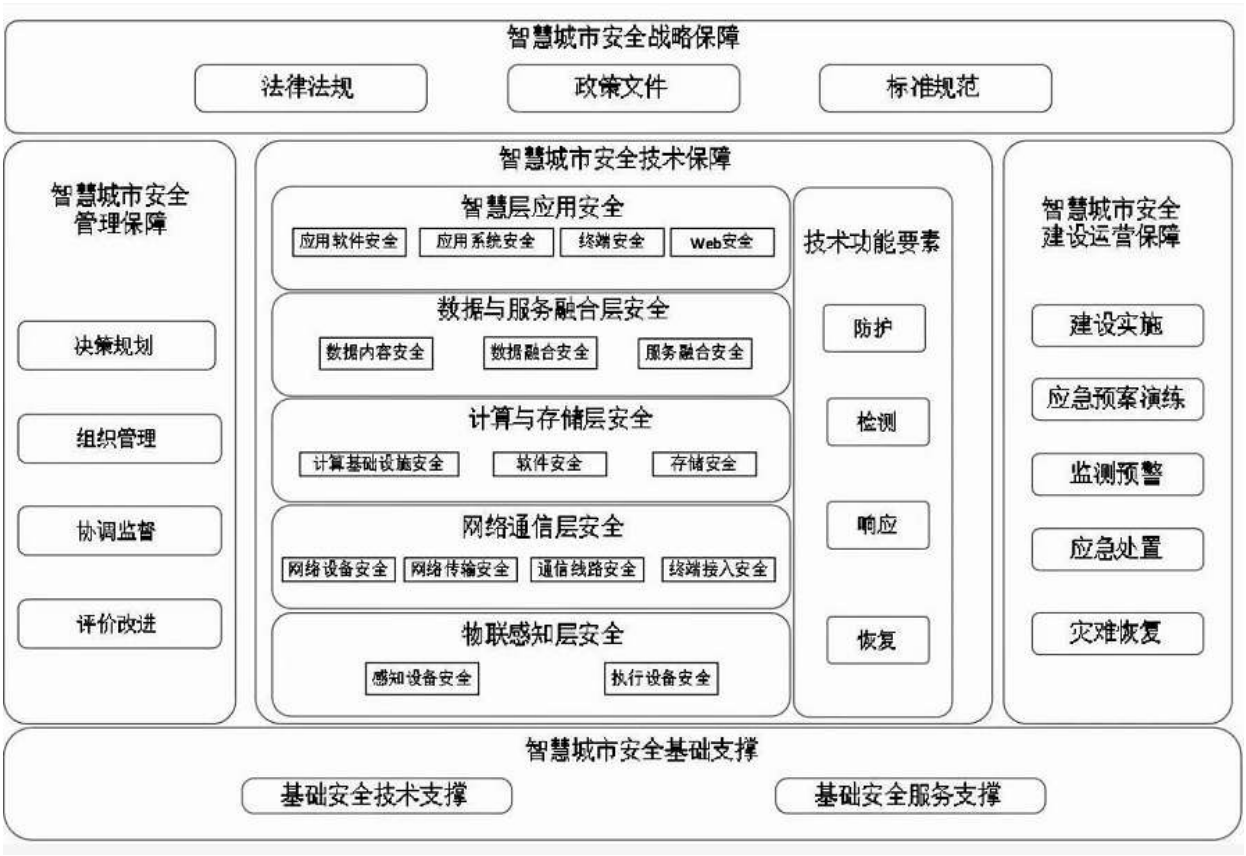


资料来源：《智慧城市评价模型及基础评价指标体系》、广证恒生

在智慧城市部署中，大量智能终端设备和传感器接入综合网络，产生复杂的接入环境、多样化的接入方式和数量庞大的智能接入终端加大了智慧城市系统的接入风险智慧城市中传感感知、通信传输、应用服务、智能分析处理等诸多层面安全风险和脆弱性日益凸显。

国家在《智慧城市评价模型及基础评价指标体系》（GB/T 34680.1-2017）中提出智慧城市安全体系框架的构建：以安全保障措施为视角，从智慧城市安全战略保障、智慧城市安全技术保障、智慧城市安全管理保障、智慧城市安全建设运营保障和智慧城市安全基础支撑五个方面给出了智慧城市安全要素。

图表 17 智慧城市安全体系



资料来源：《智慧城市评价模型及基础评价指标体系》、广证恒生

风华正茂科技 O2O 研究院提出确保智慧城市建设的十个要点：一、质量检查和渗透测试;二、在面向服务级别协议中安全性优先;三是建立计算机攻击应变小组或网络安全事件应变小组;四是确保软件更新的一致性和安全性;五是根据职能基础架构的生命周期进行规划;六是处理数据时注意保护隐私；七是公共通信通道加密、认证和管理;八、永远做好人工接手控制的准备；九、设计容错系统;十、确保基本服务的连续性。随着智慧城市建设的进一步探索，未来有望摆脱安全困扰。

2.2 智慧安防：从电子安防转型，源头上遏制安全风险的发生

2018 北京安博会释放了安防行业朝着智慧安防转型的信号，未来伴随着雪亮工程、公安大数据、智能感知网等一系列国家和地方政策的出台，安防产业有望迎来新一轮的爆发。

智慧安防系统主要包括门禁、报警和监控三大部分，主要涉及入户智能识别系统、智能门锁、智能多重安防报警系统。2017 年中国门禁系统市场规模近 170 亿元，据预测 2018 年中国门禁系统市场规模有望突破 200 亿元。

图表 18 智慧安防系统详细剖析

系统	内容	安全威胁
防盗报警系统	系统的前端设备为各种类别的报警传感器或探测器;系统的终端是显示/控制/通信设备，它可应用独立的报警控制器，也可采用采用报警中心控制台控制。	漏报警

视频监控报警系统	应用于建筑物内的主要公共场所和重要部位进行实时监控、录象和报警时的图象复核。视频监控报警系统的前端是各种摄象机、视频检测报警器和相关附属设备	仪器被黑客入侵无法记录
紧急控制系统	采用现代电子信息技术，在建筑物的出入口对人(或物)的进、出，实施放行、拒绝、记录和报警等操作的一种自动化系统。出入口目标识别系统可分为对人的认别和对物的认别。	人脸识别有误，通信系统瘫痪

资料来源：公开资料整理、广证恒生

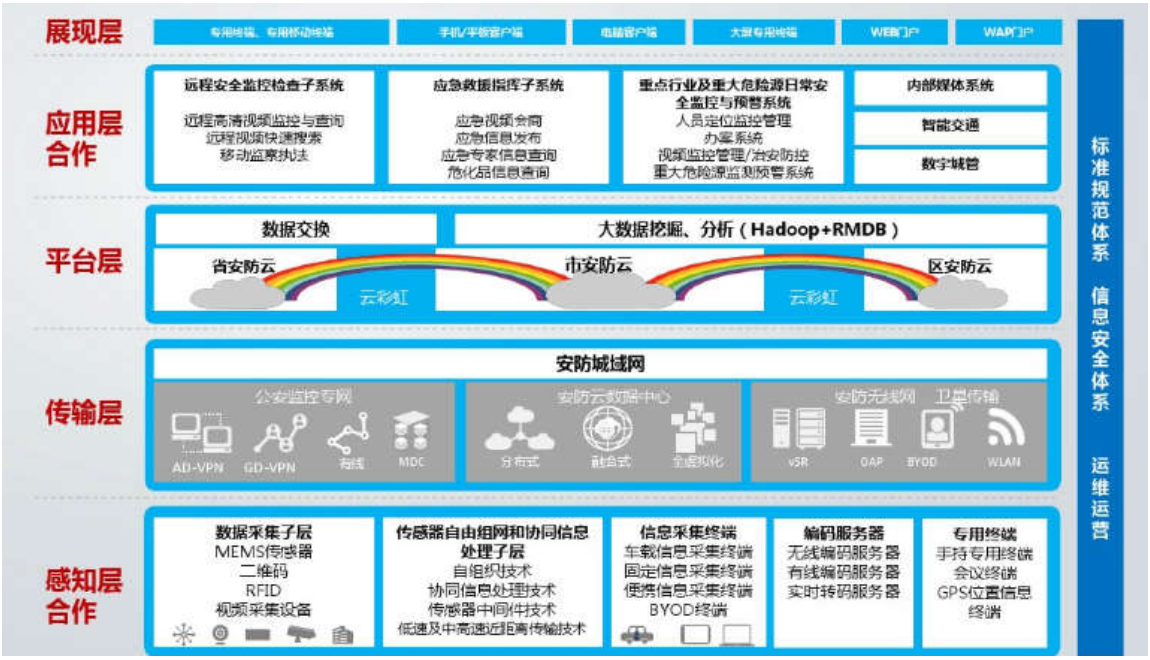
在智慧安防产业链中，上游有算法、芯片和其他零组件供应环节；中游为软硬件设备设计、制造和生产环节，主要包括前端摄像机、后端存储录像设备、音视频产品、显示屏供应商、系统集成商、运营服务商等；下游为产品分销及终端的城市级、行业级和消费级客户应用。

图表 19 智慧安防产业链

资料来源：亿欧智库、广证恒生

智慧安防的风险是劫持系统或者设备，将互联设备转化为机器人，通过监控数据源目标情报。因而在智慧安防领域中会遇到的安全问题主要在于一是监控领域，如何防止黑客进入影响监控效果；二是人脸识别技术的完善，人体密码一旦被泄露很多隐私信息也会随之而泄露。目前主要是通过层层控制，从数据源、安防领域网规范安防领域的安全构建，力求从源头上断绝给危险份子提供进入的机会。

图表 20 智慧安防安全问题解决体系



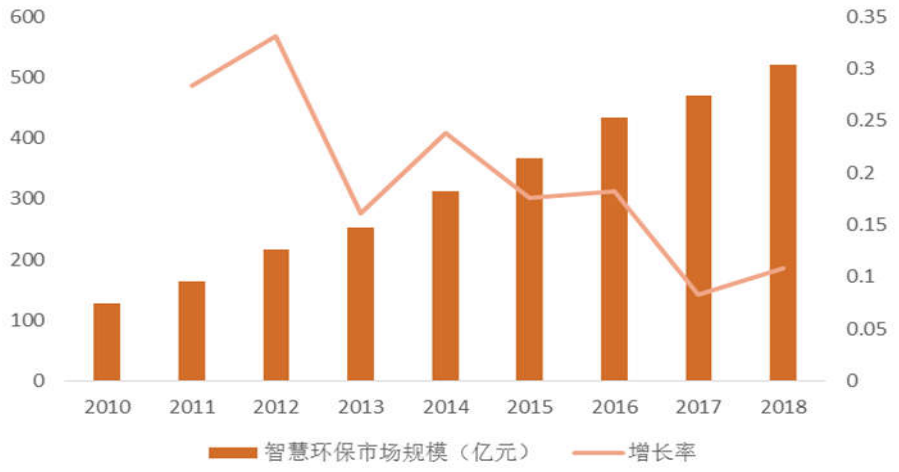
资料来源：公开资料、广证恒生

2.3 智慧环保：注重平台化的搭建，实时监控安全威胁

我国智慧环保行业发展迅速，2018 年行业规模为 521 亿元， 2010-2018 年行业复合增速达到 19.31%。与整个万亿级的环保市场相比，智慧环保的市场规模较小，未来市场增长空间巨大。

同时，“十三五”期间智慧环保行业的迅速发展主要得益于密集的政策扶持，《2018 年生态环境监测工作要点》、《生态环境监测质量监督检查三年行动计划（2018 年-2020 年）》、《环境空气质量标准》（GB 3095-2012）修改单等多部环境监测政策出台，规范促进了中国智慧环保行业的发展，智慧环保未来可期。

图表 21 2010-2018 年中国智慧环保市场规模（亿元）及增长率（%）



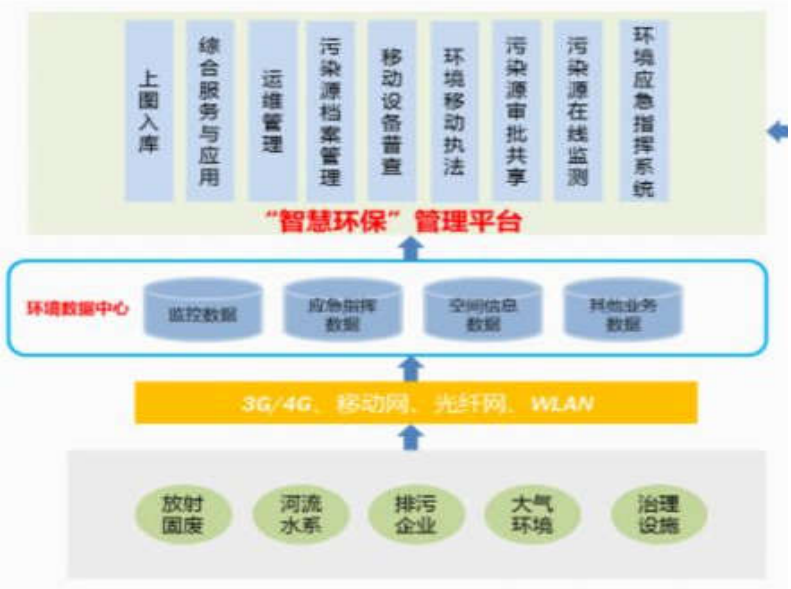
资料来源：前瞻产业研究院、广证恒生

智慧环保主要是强调感知层技术和智慧层技术的应用能够实现实时、自动化的环境数据感知系统，对环境污染源数据、大气环境质量数据等进行实时的采集和监控，同时能够通过强大的计算能力对大量环境保护监测数据进行智能分析，推动环境保护工作的智能化、自动化。

智慧环保需要建立地理信息系统、环境数据中心、综合办公系统、环境监控系统、移动在依法系统、应急指挥系统、环境信息展示与决策系统等子系统，并且辐射到各个地区和层级，构建环境信息化管理和监管执法业务体系。智慧环保主要涉及到数据采集硬件和数据中心软件系统两部分，这两块正是安全防范的重点。

目前智慧环保还在建立的过程，如何在构建的时候将安全问题考虑进顶层设计问题中是重点。政府要求试点省份力争在 2017 年 6 月底前完成试点工作，未纳入试点的省份力争在 2018 年 6 月底前完成省以下环境保护管理体制调整工作，确保“十三五”时期全面完成环保机构监测监察执法垂直管理制度改革任务，到 2020 年全国省以下环保部门按照新制度高效运行。智慧环保可以从源头上抓好安全设置的问题。

图表 22 智慧环保架构



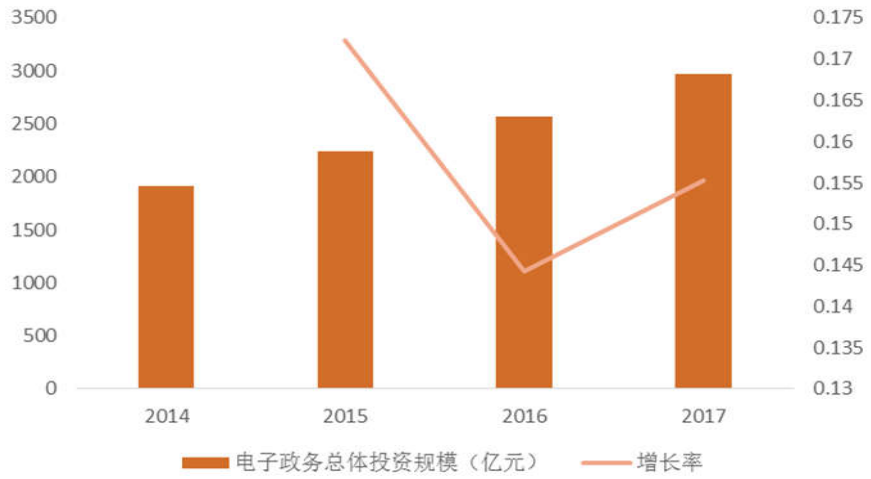
资料来源：公开资料、广证恒生

智能环境能帮助城市制定精确且高效的环境决策。其安全风险是攻击智能阀门，导致废水溢出；劫持系统设备；操纵命令并且阻碍系统响应；利用传感器跟踪活动。由于主要是攻击设备应用层，目前主流的应对方式是实时监控，注意异常事项的出现。

2.4 智慧政务：配备全方位高等级的安全防御能力

随着物联网的发展，政府业务的智能化随之崛起，物联网更好的利用政务数据服务于大众。2017 年我国电子政务总体投资规模达到 2968 亿元，未来我国电子政务市场规模仍将保持较快增长。到 2020 年，总体投资规模预计将达到 4500 亿元左右。

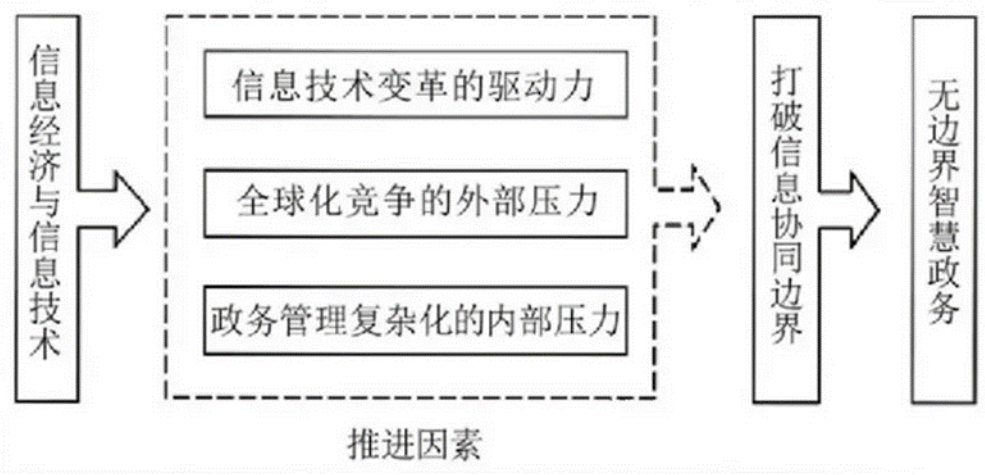
图表 23 2014-2017 年我国电子政务总体投资规模（亿元）及增长率（%）



资料来源：新思界产业研究中心、广证恒生

智慧政务云平台的建设是智慧政务建设的基础，以实现政务数据资源的归集、共享、开放、应用，努力形成标准共建、网络互通、业务协同、应用创新的智慧政务新局面。

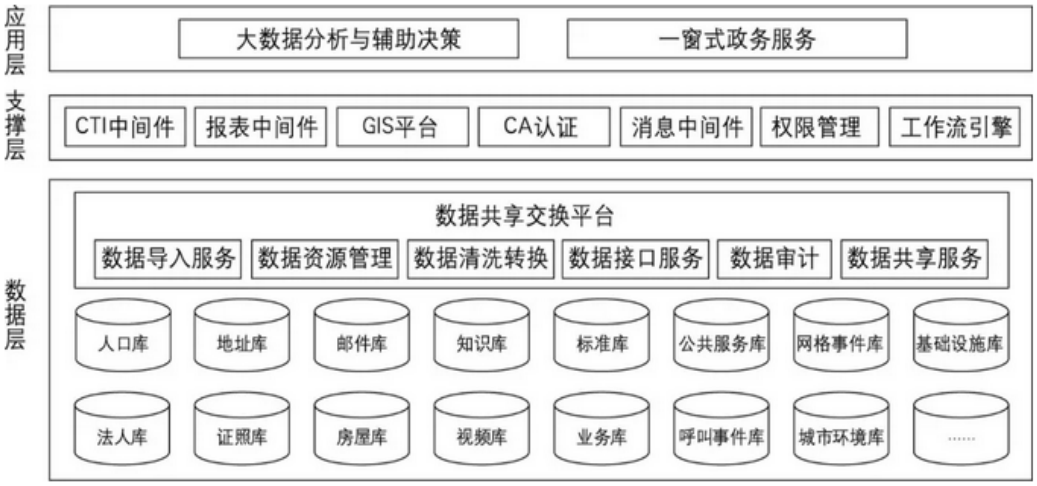
图表 24 智慧政务的推进因素



资料来源：政府官网、广证恒生

智慧政务的设计通过构建集中的数据中心，打破政府部门各业务系统间政务信息的条状分布制约，可进行社会治理业务中的数据分析与应用，以及政务服务业务中的数据沉淀、数据回填操作，打破“信息孤岛”的管理机制问题，有效解决政府政务冗杂的问题。

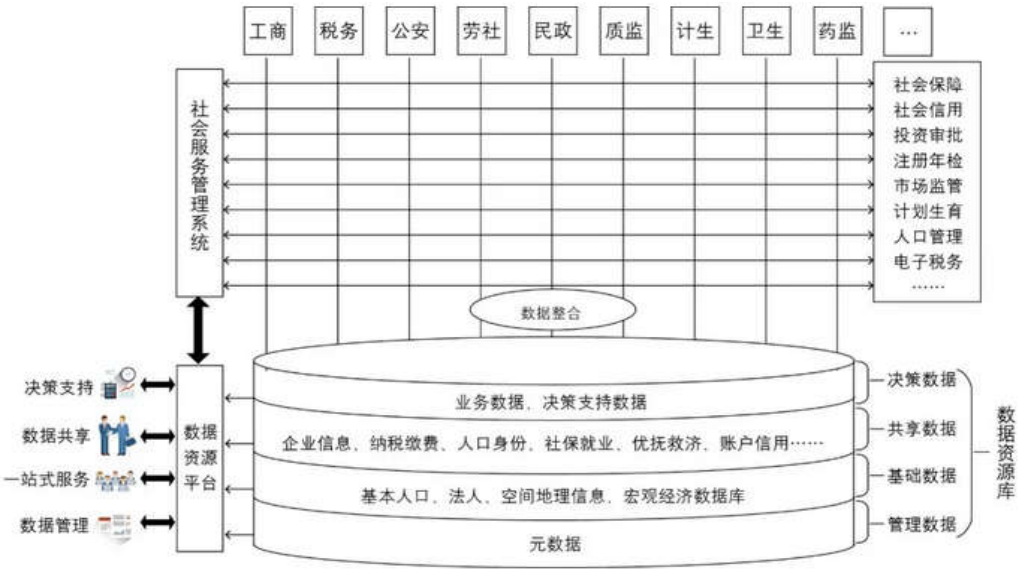
图表 25 智慧政务设计框架



资料来源：政府官网、广证恒生

数据层基于数据中心和数据交换功能进行设计，由各职能部门已有信息汇集资源构成，包括人口数据、法人数据、地理数据、电子证照数据等，为政务大数据共享与分析提供统一的数据支撑，是政务大数据进行实际应用的基础。如何保障数据的安全，防止数据泄露以防止政府工作的瘫痪这是未来最大的难题。

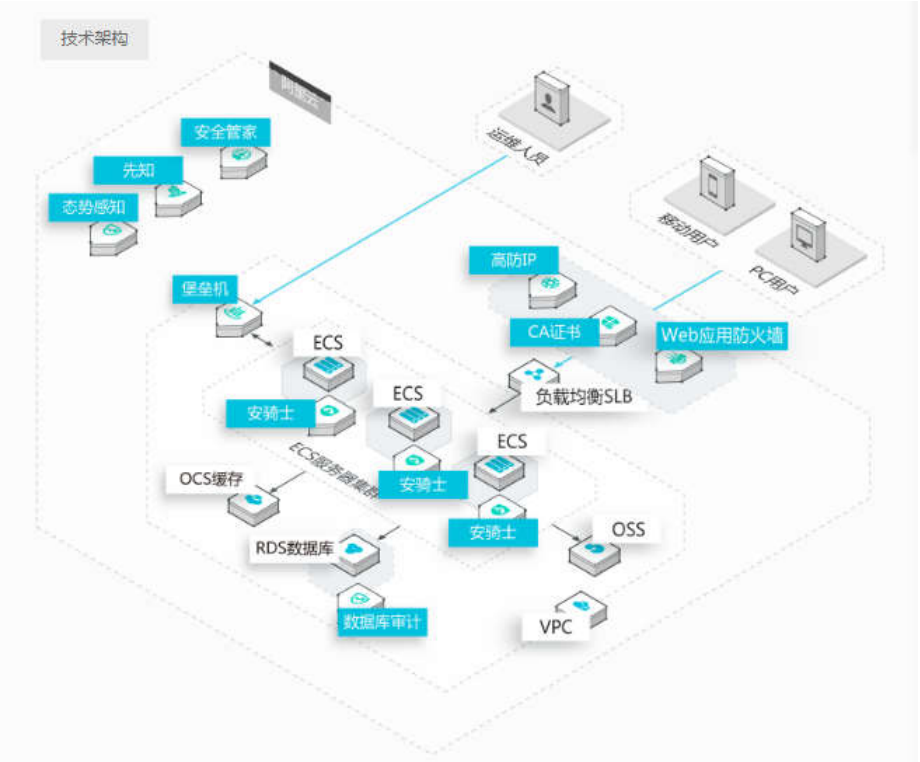
图表 26 数据资源库总体架构



资料来源：政府官网、广证恒生

政务系统安全主要面临着ISV安全开发能力不足、缺乏纵深防御体系、缺乏未知威胁监测能力以及缺乏整体持续监控能力，因此应对的方法是增加防御能力：主机安全防御能力、Web 安全防御能力、DDoS 攻击防御能力以及整体态势感知能力以提高智慧政务整体系统的安全系数。

图表 27 智慧政务安全问题解决方案框架



资料来源：阿里云、广证恒生

3、物联网设备端潜在的发展契机

3.1 深耕芯片技术研发，力求解决漏洞困扰

芯片是物联网设备中不可缺少的一环，随着物联网的崛起，芯片市场迎来新一轮增长爆发期，同时由于我国的芯片还未跻身于世界前列，芯片技术的研发一并被激起。根据预测到 2020 年我国芯片市场规模有望达到 338 亿元。

图表 28 2015-2020E 年中国物联网芯片市场规模（亿元）及增长率（%）

资料来源：公开资料、广证恒生

近几年芯片漏洞频繁发生，前有英特尔系列处理器被 Google Project Zero 团队发现的存在安全漏洞，后有计算机芯片制造商 AMD 在售的芯片存的 13 个安全漏洞被爆，涉及多款处理器。大量隐藏在芯片中的“硬件木马”如何保障物联网安全。

物联网安全芯片可以比较有效的解决安全威胁，它是一个可独立进行密钥生成、加解密的装置，内部拥有独立的处理器和存储单元，可存储密钥和特征数据，为电脑提供加密和安全认证服务。据数据统计，2011-2017 年间，我国的安全芯片市场规模增长迅速，基本保持了三成左右的增长率，其中，2017 年我国安全芯片市场接近 80 亿元。

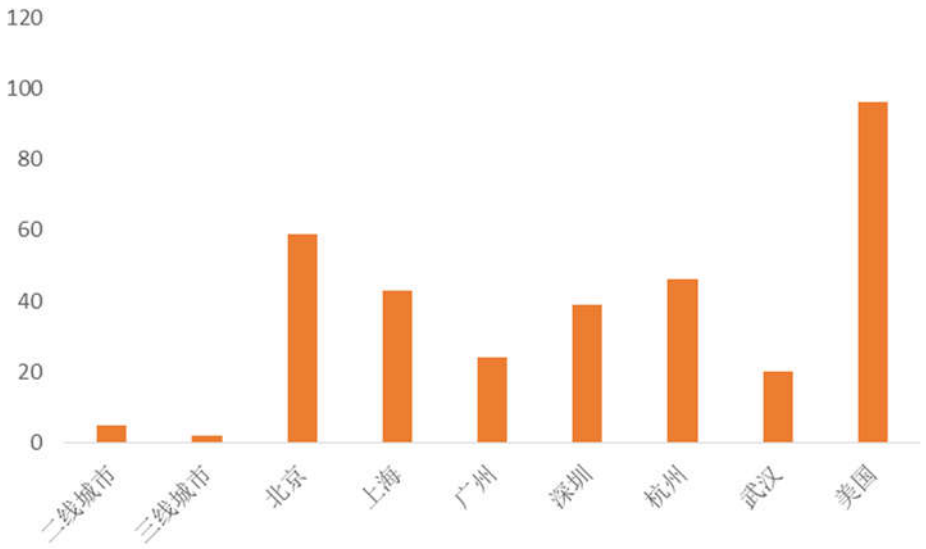
芯片级的网络安全必须以 EDA 工具为核心，从三个设计层次着手。首先是芯片层面的跨频道攻击防护策略，其次是供应链的安全管理机制，第三则是芯片内部逻辑单元的木马侦测能力。通过层层把关 IP 和逻辑安全，防止未经验证及授权的芯片流入市面，让制造商能全面掌握设计问题，来确保物联网应用的安全。

在 ISC 2018 中国互联网安全大会上，岳超提出物联网安全芯片是具有安全密码功能和片上存储功能的 SOC 芯片，在安全硬件的基础设施上，搭载了安全的平台系统以及安全应用。它提供系统可信根、数据安全存储，保障安全运行以及安全连接，从硬件层面对智能终端产品进行了完整保护。

3.2 安全管理+技术双管齐下，消除隐藏在摄像头的安全隐患

我国摄像头渗透率最高的城市是北京，每一千人有 59 个，然而与美国相比还是有一定的差距，美国是每一千人有 96 个，因而我国摄像头仍有很大的市场空间。

图表 292017 年摄像头渗透率（个/千人）

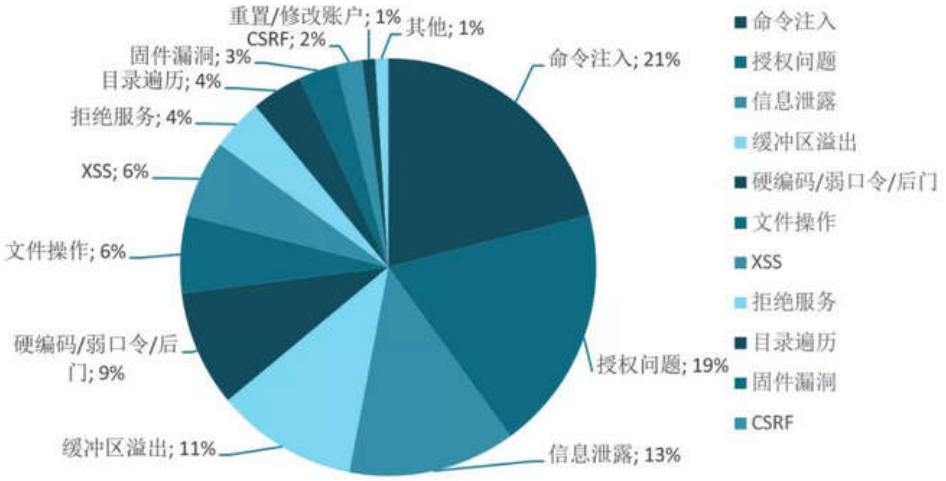


资料来源：中国统计局、广证恒生

摄像头的广泛使用，有助于提高城市监控无死角能力，减少犯罪违法行为。然而摄像头潜藏着无穷的安全隐患：2016 年底，数十万摄像头组成的僵尸网络 Mirai，以当时最大(620G)DDoS 流量，攻击美国域名服务商 Dyn，导致多家知名网站无法访问。

摄像头存在的安全隐患主要集中在两个方面：一是大量摄像头组成的网络被黑客入侵;二是摄像头采集视频被攻击者控制后，易发生隐私泄漏。其存在的漏洞类型包括命令注入、授权、信息泄露、缓冲区溢出、弱口令、文件操作、XSS、拒绝服务、目录遍历、固件漏洞等。

图表 30 摄像头存在的漏洞类型



资料来源：《网络空间测绘系列——2018 年摄像头安全报告》、广证恒生

《网络空间测绘系列——2018 年摄像头安全报告》中提出若要从根本上解决摄像头安全问题，需以安全管理和安全技术相结合。在管理方面，要建立摄像头的相关安全标准，把摄像头纳入网络资产，进行

统一化的安全管理。技在术方面，制造商需要加强安全意识、建立那倒安全开发流程，并对产品进行检查和跟踪等。安全厂商则要从防护、检测、网络、通讯、硬软件等多个维度为用户提供合适的安全解决方案。随着我国的摄像头进一步安置，安全问题可以随之考虑，未来物联网安全下的摄像头安全隐患有望一次性彻底解决。

3.2 以“加密”为核心抵御云平台的瘫痪

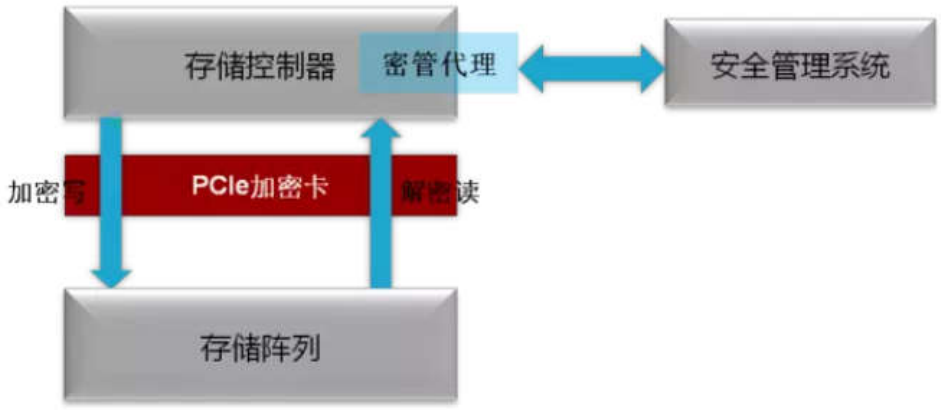
在物联网的应用层，云平台是实现用户运用的重要阶段。从功能角度看，物联网云平台主要包含CMP（连接管理）、AEP（应用使能）、DMP（设备管理）和BAP（业务分析）四大功能。物联网的云平台出现的安全威胁主要在数据存储、访问以及传输过程中。云对象存储需要在数据安全、数据完整性、身份认证、数据访问控制、数据机密性及内存删除等多方面保证用户数据的安全。

图表 31 物联网云平台按功能的分类

资料来源：公开资料、广证恒生

数据传输的安全主要通过加密进行，实现加密储存，依赖于安全存储系统，安全存储系统包括四个部分：存储阵列、 PCI 加密卡、安全管理中心、密管代理。

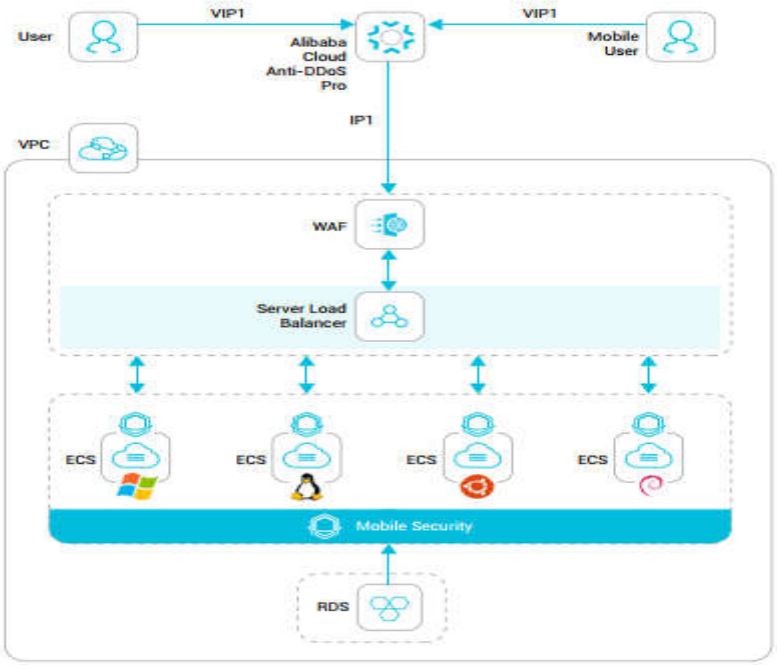
图表 32 数据加密储存体系结构



资料来源：公开资料、广证恒生

在物联网云平台安全方面，阿里云提供种类齐全的安全解决方案包括 DDoS 安全防护、Web 应用防火墙、移动安全和访问管理。当出现新的威胁时阿里云有专门的安全研发团队提供解决方案，力求用更卓越的 DDoS 防护和 WAF 支持使安全逻辑更坚固。再者平台已经接受了私人设备与工作设备之间的模糊界线目前的 IT 生态系统不再局限于其内部基础设施极大拓宽了设备的安全使用范围。

图表 33 阿里云平台安全解决方案图解



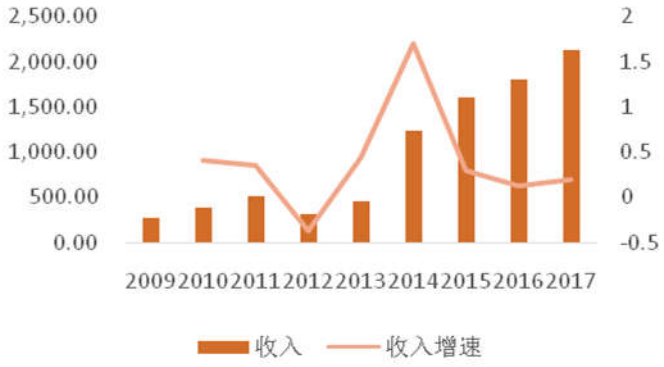
资料来源：阿里云官网、广证恒生

4、相关标的

4.1 卫士通(002268.SZ)：密码产品+信息安全产品+安全信息系统，全方位领跑物联网安全领域

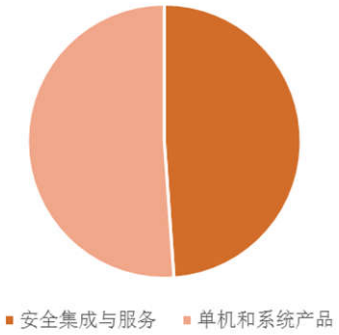
公司深耕信息安全领域，形成密码产品、信息安全产品、安全信息系统三大信息安全产品体系。并且公司和控股股东中国网安都提前布局物联网安全，子公司嘉微在 2016 年就已针对物联网安全这个方向着重进行了战略安排，成立了一支由 40 位核心骨干人员组成的研发力量，目前，嘉微公司已经形成了四个系列的物联网相关的产品，在 2018 年整个业务产值已经达到了两个亿。公司借着本身在信息安全领域的产品优势，继续在物联网安全领域是处于行业领先的地位。

图表 342009-2017 年卫士通的收入（百万元）及增速



资料来源：公司年报、广证恒生

图表 35 2017 年卫士通业务拆分情况



资料来源：公司年报、广证恒生

公司在物联网安全方面的核心竞争力主要体现在其全方位的产品系列，从密码产品到信息安全产品再到安全信息系统。

在密码产品方面，公司研发的云服务器密码机已获得商密资质，目前启动了移动终端安全芯片和龙芯安全相关产品的研制；同时密码服务平台软模块、Win10 操作系统相关密码产品的研制均通过了相关资质鉴定。

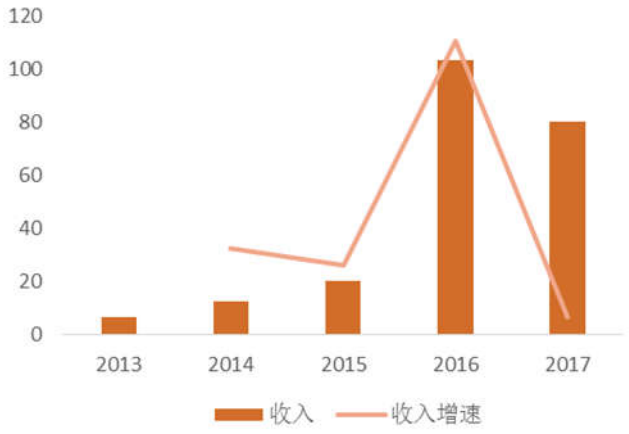
在信息安全产品方面，涵盖网络安全、主机安全、数据安全、安全应用及安全管理等多个领域。公司的安全网关产品已完成公安部资质测评、保密局对标测试以及系列 VPN 产品已完成研发。

在安全信息系统方面，公司宽带集群通信加密系统已正式上线并稳定运营；数字移动通信系统已完成定型试验、密测、软测等；安全电子邮件一期建设已经具备 15 万级用户运营服务的支撑能力；商用移动办公系统已获得公安部相关资质和软件著作权，V2.0 版本已在某省政府及卫士通移动办公系统中使用。

4.2 中宇万通(835539.OC)：商用密码技术多年积淀，走在物联网安全前端

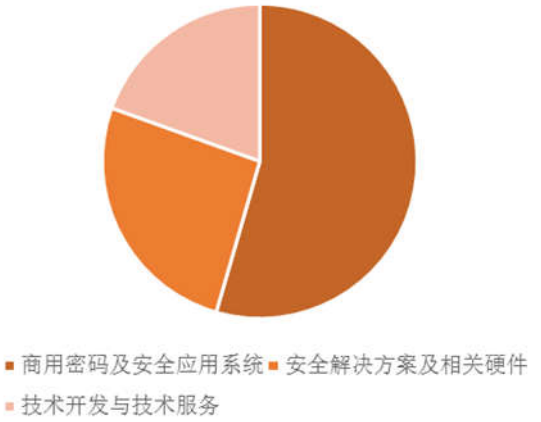
公司的主营业务是销售商用密码产品和安全应用系统产品以及提供信息安全解决方案。公司的商用密码产品 TrustMore 安全网关系列产品相比于市场上提供安全网关产品具有系统整合性高、维护便捷的特点，成为公安、外交及政府部门边界接入平台建设的重要组成部分。2017 年公司营业收入实现营业收入 80,03.73 万元，同比减少 22.53%，但是净利润为 20,07.21 万元，同比增长 50.27%。

图表 362013-2017 年中宇万通的收入（百万元）及增速



资料来源：公司年报、广证恒生

图表 37 2017 年中宇万通业务拆分情况



资料来源：公司年报、广证恒生

在物联网安全领域逐渐崛起之时，公司坐拥三大优势：技术、客户和产品，有望趁势再赢新一轮的增长。在技术方面公司拥有强大的研发实力,专注于信息安全领域,自主研发推出了一系列商用密码产品，涵盖了多个领域包括可信安全接入、集中认证、移动安全接入、金融 PBOC 在线安全支付、物联网安全数据采集、安全文件共享、移动终端安全认证、视频安全准入、数字签名验签和时间戳服务等。在客户方面公司与政府、金融和大型央企等保持着长期稳定的合作关系。在产品方面，公司 2017 年新研发智能安全应用网关 V1.0 将传统协议与安全协议有机结合、同时适应大流量的视频应用场景和传统业务需要；再者公司研发全系列商用密码产品可以部署于云计算虚拟化环境中，而该产品的独立传统平台版本已经比传统产品性能提升了 10 倍以上，走在行业的前端。

再者公司新研发了安全准入系统、智能安全应用网关、驾考安全管理系统等应用安全产品。并且公司于 2018 年 5 月与方正国际签订重大战略协议，形成一系列全方位基于密码技术的安全防护、安全应用类产品和解决方案，强势进军物联网安全领域，为行业提供安全保障一条龙服务。

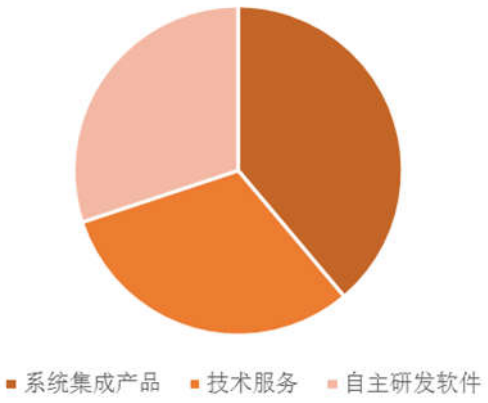
4.3 优炫软件(430208.OC):专注于数据安全防护，受益于物联网安全市场增长

公司专注于为用户提供多层次的核心数据安全防护产品，产品体系涉及操作系统安全、数据库安全、业务安全、运维安全、大数据安全以及云数据库等六大领域，为物联网安全首先出现的数据问题提供接触安全威胁的方案。2017 年公司营业收入为 3.30 亿元，同比增长 55.49%；主营业务主要为系统集成产品（38.85%）、技术服务（31.07%）和自主研发软件（30.08%）。

图表 382010-2017 年优炫软件的收入（百万元）及增速

资料来源：公司年报、广证恒生

图表 39 2017 年优炫软件业务拆分情况



资料来源：公司年报、广证恒生

在物联网安全领域中，公司的核心竞争力主要体现着在技术、产品和渠道三个方面：公司拥有非专利技术优炫 RS-CDPS 核心数据安全保护技术及基于 CA 证书的身份认证机制、基于操作系统驱动级的安全管理机制、细粒度的权限控制技术、系统自我保护技术共 11 项专利技术，深耕安全防护方向。在产品方面，公司的防护能力走在行业前列，核心数据保护系列产品是针对操作系统和数据库核心层的安全增强产品，能够有效防范对核心层或从内部发起的攻击；另一款基础软件优炫云数据库（UXDB）是一款成熟的基于 NewSQL 适应云平台环境的数据库系统。在渠道方面，公司在全国重点区域和主要省会城市均已建立分支机构，并采取“销售产品+技术服务”的盈利模式，力求实现在全国范围内对于客户需求的第一时间响应，为客户提供信息安全的解决方案，快速解决威胁是物联网所需的重要防御能力。

5、风险提示

（1）物联网安全行业发展不达预期的风险

物联网安全行业仍处于成长期，目前我国网络安全方面的投入占整个IT比重仅约2%，远低于欧美国家10%左右的水平，预计恶性安全事件将刺激物联网安全市场发展。

（2）技术进步发展不达预期的风险

物联网安全的实现需要依靠技术的进步，黑客也在不停地寻找漏洞，很有可能出现新的不可预料的威胁，没有足够的技术无法解决所发现的安全漏洞，容易导致整个物联网产业的崩溃。

新三板团队介绍：

在财富管理和创新创业的两大时代背景下，广证恒生新三板构建“研究极客+BANKER”双重属性的投研团队，以研究力为基础，为企业量身打造资本运营计划，对接资本市场，提供跨行业、跨地域、上下游延伸等一系列的金融全产业链研究服务，发挥桥梁和杠杆作用，为中小微、成长企业及金融机构提供闭环式持续金融服务。

团队成员：

袁季（广证恒生总经理兼首席研究官）：长期从事证券研究，曾获“世界金融实验室年度大奖—最具声望的 100 位证券分析师”称号、2015 及 2016 年度广州市高层次金融人才、中国证券业协会课题研究奖项一等奖和广州市金融业重要研究成果奖，携研究团队获得 2013 年中国证券报“金牛分析师”六项大奖。2014 年组建业内首个新三板研究团队，创建知名研究品牌“新三板研究极客”。

赵巧敏（新三板研究总监、副首席分析师）：英国南安普顿大学国际金融市场硕士，8 年证券研究经验。具有跨行业及海外研究复合背景，曾获 08 及 09 年证券业协会课题二等奖。具有多年 A 股及新三板研究经验，熟悉一二级资本市场运作，专注机器人、无人机等领域研究，担任广州市开发区服务机器人政策咨询顾问。

温朝会（新三板副团队长）：南京大学硕士，理工科和经管类复合专业背景，七年运营商工作经验，四年市场分析经验，擅长通信、互联网、信息化等相关方面研究。

黄莞（新三板副团队长）：英国杜伦大学金融硕士，具有跨行业及海外研究复合背景，负责教育领域研究，擅长数据挖掘和案例分析。

司伟（新三板高端装备行业负责人）：中国人民大学管理学硕士，理工与经管复合专业背景，多年公募基金从业经验，在新三板和 A 股制造业研究上有丰富积累，对企业经营管理有深刻理解。

魏也娜（新三板 TMT 行业高级研究员）：金融硕士，中山大学遥感与地理信息系统学士， 3 年软件行业从业经验，擅长云计算、信息安全等领域的研究。

刘锐（新三板医药行业高级研究员）：中国科学技术大学有机化学硕士，具有丰富的国内医疗器械龙头企业产品开发与管理经验，对医疗器械行业的现状与发展方向有深刻的认识，重点关注新三板医疗器械、医药的流通及服务行业。

胡家嘉（新三板医药行业研究员）：香港中文大学生物医学工程硕士，华中科技大学生物信息技术学士，拥有海外知名实业工作经历，对产业发展有独到理解。重点研究中药、生物药、化药等细分领域。

田鹏（新三板教育行业研究员）：新加坡国立大学应用经济学硕士，曾于国家级重点经济期刊发表多篇论文，具备海外投资机构及国内券商新财富团队丰富研究经历，目前重点关注教育领域。

于栋（新三板高端装备行业高级研究员）：华南理工大学物理学硕士，厦门大学材料学学士，具有丰富的一二级研究经验，重点关注电力设备及新能源、新材料方向。

史玲林（新三板大消费&教育行业研究员）：暨南大学资产评估硕士、经济学学士，重点关注素质教育、早幼教、母婴、玩具等消费领域。

李嘉文（新三板主题策略研究员）：暨南大学金融学硕士，具有金融学与软件工程复合背景，目前重点关注新三板投资策略，企业资本规划两大方向。

联系我们：

邮箱：huangguan@gzgzhs.com.cn

电话：020-88832319

广证恒生：
地址：广州市天河区珠江西路 5 号广州国际金融中心 4 楼
电话：020-88836132，020-88836133
邮编：510623

股票评级标准：
强烈推荐：6 个月内相对强于市场表现 15%以上；
谨慎推荐：6 个月内相对强于市场表现 5%—15%；
中性：6 个月内相对市场表现在-5%—5%之间波动；
回避：6 个月内相对弱于市场表现 5%以上。

分析师承诺：

本报告作者具有中国证券业协会授予的证券投资咨询执业资格，以勤勉的职业态度，独立、客观地出具本报告。本报告清晰、准确地反映了作者的研究观点。在作者所知情的范围内，公司与所评价或推荐的证券不存在利害关系。

重要声明及风险提示：