安博通(688168)

国内先进的网络安全企业

分析日期 2019 年 08 月 22 日

投资评级：中性/首次

证券分析师：黄伯乐

执业证书编号：S0630516070001

电话：021-20333213

邮箱：hbl@longone.com.cn

◎主要观点：

◆**国内先进的网络安全企业。**公司主营业务为网络安全核心软件产品的研究、开发、销售以及相关技术服务，为网络安全行业网络安全系统平台与安全服务提供商。安博通坚持核心技术自主创新，是网络安全能力输出者、上游软件平台与技术提供商，公司将网络安全产品与服务提供给各大产品与解决方案厂商，由合作伙伴交付给政府与企事业单位等最终用户，是网络安全行业“厂商的厂商”。

◆**公司营收和净利润保持较快增长。**公司营业收入和净利润增速较快。2016-2018 年，公司营收分别为 1.06 亿元，1.51 亿元和 1.95 亿元，2016 年到 2018 年的增速分别为 73.87%，41.77%和 29.58%；归属母公司股东的净利润分别为 0.19 亿元， 0.35 亿元和 0.60 亿元，2016 年到 2018 年的增速分别为 39.47%，80.13%和 73.51%。

◆**公司技术研发实力突出。**公司通过持续的技术创新，截至本招股说明书签署日，公司已申请发明专利共 109 项，其中 12 项已取得发明专利证书，拥有计算机软件著作权 74 项，已形成了具有自主知识产权的核心技术和知识产权体系。

◆**公司拥有优质的客户基础。**经过多年发展，公司积累了一大批行业内知名客户，包括华为、新华三、星网锐捷、卫士通、启明星辰、360 网神、任子行、绿盟科技、太极股份、荣之联、中国电信系统集成、迈普通信等知名产品与解决方案厂商。

◆**公司拥有快速的上游技术响应和服务。**公司设置专业的售前售后技术服务部门，团队深入客户业务场景了解和传递需求，为用户提供技术指导和支撑，产品和研发部门快速响应需求，使得产品快速迭代创新，支撑客户快速多变的业务发展。

◆**募集资金用途。**公司拟向社会公开发行不超过 1,279.50 万股，占发行后总股本的比例不低于 25%。发行后总股本不超过 5,118.00 万股。公司本次实际募集资金扣除发行费用后的净额将全部投资于以下项目：深度网络安全嵌入系统升级与其虚拟资源池化项目，安全可视化与态势感知平台研发及产业化项目和安全应用研发中心与攻防实验室建设项目。

◆**盈利预测：**根据行业的空间和公司的主要优点，预计公司 2019-2021 年总体收入分别为 2.51、3.12 和 3.86 亿元，同比增速为 28.03%、24.81%和 23.55%；归母净利分别为 0.71、0.90 和 1.15 亿元，同比分别增长 15.76%、36.80%、30.59%。以发行后总股本 0.512 亿股计算，2019-2021 年 EPS 分别为 1.39、1.77 和 2.25 元。参考对比公司启明星辰和绿盟科技最近的 PE（TTM）值，我们建议以 2019 年对应 EPS 的 30-40 倍左右 PE 申购，申购价格大概为 41.75-55.66 元/股。

◆**风险提示**

产品集中风险，应收账款风险。

正文目录

图表目录

1.公司基本情况

1.1.公司的发展历程

安博通有限成立于2007年5月25日,法定代表人为郑书群,注册资本为50.00万元,设立时公司名称为北京永顺达文化传播有限公司（后于2011年8月1日名称变更为北京安博通科技有限公司）。2007年5月25日，北京富尔会计师事务所有限责任公司出具“京富会（2007）2-100号”《开业登记验资报告》，验证截至2007年5月24日止，安博通有限已收到全体股东货币出资。2007年5月25日，安博通有限取得北京市工商行政管理局宣武分局核发的《企业法人营业执照》（注册号：110104010226475）。

2016年5月4日，安博通有限股东会审议通过将有限责任公司整体变更为股份有限公司的决议。根据大信会计师事务所（特殊普通合伙）2016年4月27日出具的大信审字[2016]第27-00047号《审计报告》，以安博通有限经审计的2016年3月31日账面净资产46,394,810.86元为基准，按照1：0.1724331的折股比例折为8,000,000.00股，每股面值1元。整体变更设立后的公司注册资本为8,000,000.00元，剩余净资产38,394,810.86元转作公司的资本公积。2016年6月23日，安博通有限在北京市工商局西城分局完成整体变更为股份公司的工商变更登记手续，并取得统一社会信用代码为91110108663136638D的《营业执照》。

2016年11月8日，公司正式在股转系统挂牌并公开转让，转让方式为协议转让，证券代码为839570，证券简称“安博通”。2019年2月28日，公司取得股转系统出具的《关于同意北京安博通科技股份有限公司股票终止在全国中小企业股份转让系统挂牌的函》(股转系统函【2019】678号)，同意公司股票自2019年3月5日起在全国中小企业股份转让系统终止挂牌。

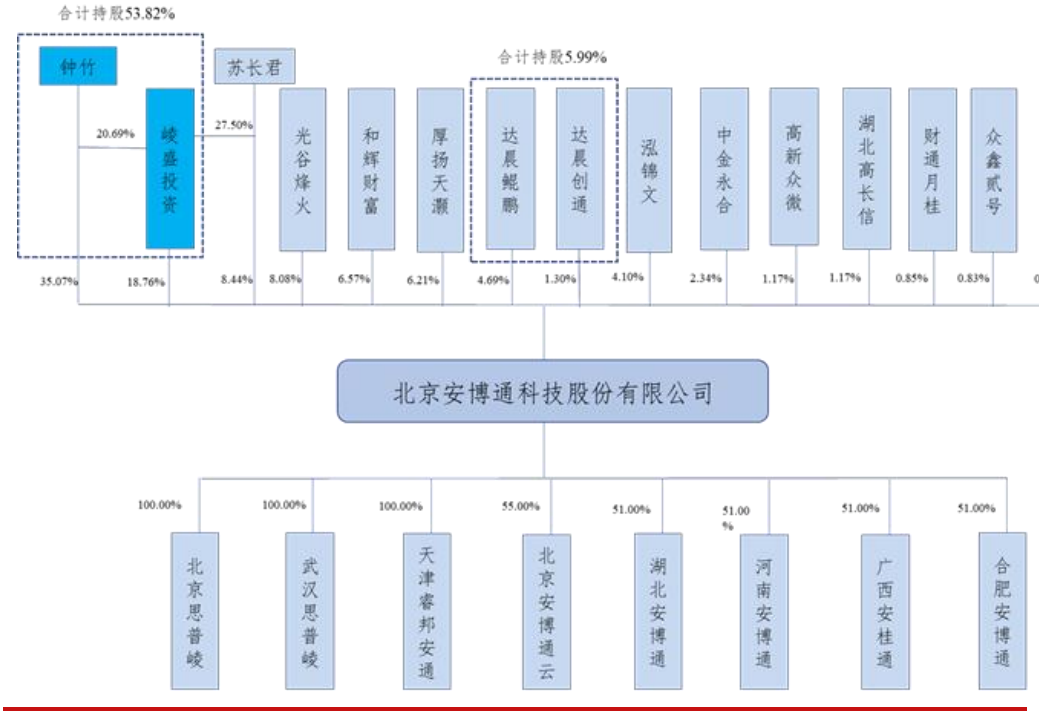
经过多次增资扩股和股权转让，形成上市前的股权结构。

1.2.股权比较中

钟竹直接持有公司13,460,000股，占公司股本总额的35.07%；通过崚盛投资间接持有公司1,489,496股，占公司股本总额的3.88%，钟竹直接和间接合计持有公司股份14,949,496股，占股本总额的比例为38.95%。同时，钟竹通过崚盛投资控制公司表决权占总表决权比例为18.76%，直接及间接控制公司表决权占总表决权比例为53.82%，为公司的控股股东及实际控制人。

本次发行前公司总股本为3,838.50万股，本次拟发行人民币普通股不超过1,279.50万股，占发行后总股本的比例不低于25%，本次发行后公司总股本不超过5,118.00万股。

图 1　发行上市前公司股权结构



资料来源：公司招股说明书，东海证券研究所

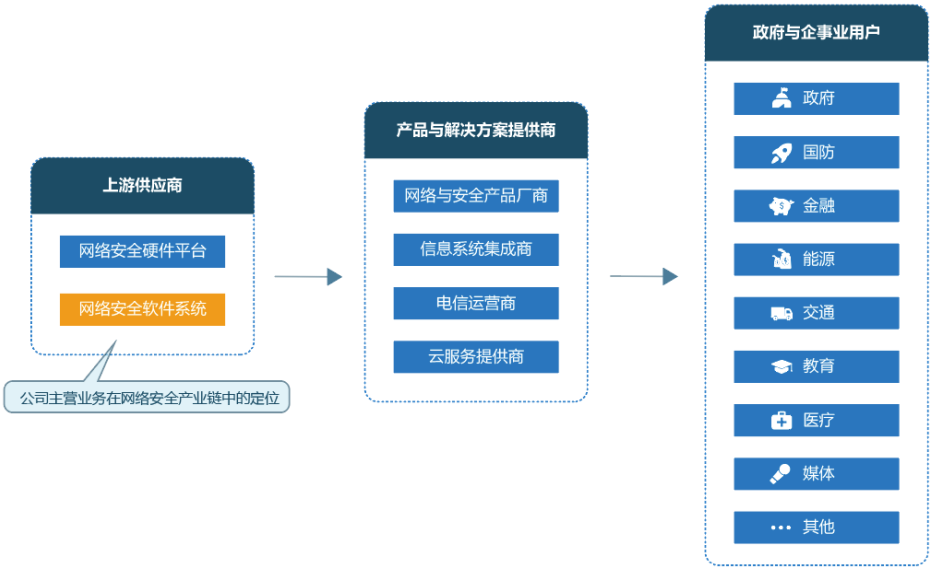
1.3.公司的主营业务

公司主营业务为网络安全核心软件产品的研究、开发、销售以及相关技术服务，为网络安全行业网络安全系统平台与安全服务提供商。在网络安全行业中，公司依托于自主开发的应用层可视化网络安全原创技术，为业界众多网络安全产品提供操作系统、业务组件、分析引擎、关键算法等软件产品及相关的技术服务。

安博通坚持核心技术自主创新，把业务聚焦到自身擅长的技术研发领域，是网络安全能力输出者、上游软件平台与技术提供商，公司将网络安全产品与服务提供给各大产品与解决方案厂商，由合作伙伴交付给政府与企事业单位等最终用户，是网络安全行业“厂商的厂商”。

公司主营业务在网络安全产业链中的定位如下图。

图 2 公司在网络安全产业链中的定位



资料来源：公司招股说明书，东海证券研究所

公司研发的网络安全系统平台 ABT SPOS 针对新型网络攻击手段与高级持续性威胁，具备丰富的应用层安全识别与流量解析功能，运用安全大数据分析、深度机器学习与流量可视化技术，发现并阻断网络中传统技术无法检测出的违规行为与未知威胁，已成为行业内多家大型厂商安全网关类产品和安全管理类产品所广泛选用的软件系统平台，是国内部分政府部委与央企网络安全态势感知整体解决方案的重要功能组件与数据引擎。

安博通网络安全系统平台 ABT SPOS 具备跨硬件平台适应能力与云计算虚拟化能力，全面的对外开放接口以及大规模的行业应用实践。网络产品厂商、解决方案厂商、电信运营商、云服务提供商等合作伙伴均可基于该软件快速开发各种网络安全网关类硬件设备、云环境下虚拟化安全网关、安全监测预警与运维管理类产品，从而快速响应用户需求。该平台不仅可以应用在传统计算机网络与虚拟化云计算网络中，还可以应用于 IPv6 互联网、工业互联网、视频监控网络、IoT 物联网等下一代信息网络中，同时在国产自主可控的设备网络中也有多种专业用途。其在网络安全技术与产品全景图中的定位如下图所示。

图 3 安博通网络安全系统平台的定位

资料来源：公司招股说明书，东海证券研究所

传统网络安全防御架构主体上依赖于封闭型软硬件一体化设备，安全防护系统与硬件实体紧耦合，安全能力如同“茧中蛹”一样被牢牢的束缚在各类封闭的硬件“盒子”中，无法快速灵活地部署于各类云计算虚拟化环境、各类不同架构的网络通信平台与各类物联网智能硬件场景，因此难以响应数字化时代层出不穷的安全防护需求。安博通基于自身技术的长期积累以及对客户需求的深入研究，自主研发并推出了集安全防御和安全监测功能于一体的网络安全系统平台。

公司以 ABT SPOS 平台为基础，通过持续的研发与创新，应用于网络安全防御控制、网络监测预警等领域，形成了一系列网络安全产品，主要包括安全网关产品和安全管理产品两大类。同时公司围绕 ABT SPOS 平台提供相应的网络安全技术开发与安全运维等服务。公司主要产品与服务如下表所示：

表 1 公司业务分类

业务分类		服务与名称	产品与服务概述
网络安全产品	安全网关产品	嵌入式安全网关	应用于数据通信网络的下一代防火墙产品及网络行为管理与审计产品。以嵌入式网络通信平台为硬件载体，通过解析网络流量中的用户、应用和内容等信息，为用户提供应对入侵防御和实时攻击、病毒拦截能力，并通过记录及审计用户的网络行为与内容，为企业网络优化和规划提供决策支持，为客户构建有序、健康的网络环境。
		虚拟化安全网关	应用于云计算环境的虚拟化安全网关产品，包括虚拟化下一代防火墙产品及网络行为管理与审计产品，以通用服务器为硬件载体，为云计算环境提供高扩展性、适应性以及全面的虚拟化安全能力。
	安全管理产品		大型网络与云计算环境下的网络安全管理平台。基于大数据分析与可视化技术，通过云端平台对安全设备和安全事件提

		供集中部署、运维监测、数据收集分析以及预警处置等功能。
网络安全服务		基于用户场景与个性化需求提供的差异化安全技术开发与安全运维服务

资料来源：招股说明书，东海证券研究所

公司提供的产品或服务在网络安全行业中的业务范围如下：

图 4 公司的业务范围

来源：中国网络安全产业联盟

资料来源：公司招股说明书，东海证券研究所

1.3.1. 网络安全产品

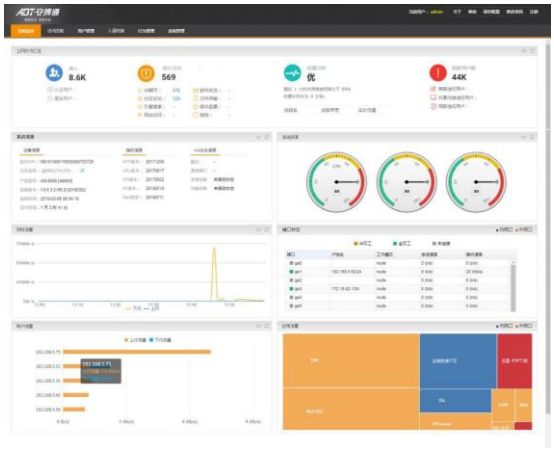
公司网络安全产品主要分为安全网关和安全管理两大类。公司在自主研发的网络安全系统平台 ABT SPOS 的基础上推出了一系列面向传统数据通信网络与云计算虚拟化环境的安全网关产品，包含嵌入式安全网关和虚拟化安全网关产品；还包括基于大数据分析及可视化技术的安全管理类产品等。各产品主要情况如下：

（1）安全网关产品

仅依靠传统的、单一功能的安全产品很难实现完整的网络安全防御体系，用户需要能够面向行业场景的、有效解决个性化需求的网络安全整体解决方案。

ABT SPOS 系统平台集成了网络安全防御过程中涉及到的网络层访问控制、应用层防火墙、入侵防御、病毒拦截、行为管理、网络审计、流量分析、威胁情报等关键要素与手段，融合到统一的安全网关平台中，用体系化的防御思路解决网络中新型的攻击与窃密行为。

图 5 公司安全网关产品界面



资料来源：公司招股说明书，东海证券研究所

1) 嵌入式安全网关

嵌入式安全网关主要用于数据通信网络环境，是一种软硬件结合的实体安全设备，通常用于网络互联网出口或网络关键区域边界，是网络中用于隔离、控制、防御的基础安全产品，在网络中的部署位置如下图所示：

图 6 嵌入式安全网关在网络中的部署位置

资料来源：公司招股说明书，东海证券研究所

嵌入式安全网关包括下一代防火墙及网络行为管理与审计等组件与产品。

下一代防火墙产品采用先进的高性能并行架构，保障业务处理高效可靠，场景支撑灵活全面。产品具备应对高级持续性威胁的入侵防御能力和实时病毒拦截技术，将访问控制模块与漏洞扫描、Web 防护、入侵防御、沙箱仿真、数据防泄漏、威胁情报等系统形成智能的策略联动，通过并行处理的深度安全检测引擎和应用识别技术，实现对用户、应用和内容的攻击行为深入分析，为用户提供安全智能的一体化防护体系。

网络行为管理与审计产品提供全网终端统一管控功能，具备传统认证和主流社交软件等身份认证方式，保障用户接入安全可控。该产品内置千万条 URL 库和五千条主流应用行为特征库，配合网络行为管理策略模板，可实现网络行为精细化识别和控制。该产品通过智能流量管理特性，动态分配空闲时带宽资源，帮助用户提升用户上网体验。该产品结合清晰易用的管理日志功能，为企业提供全面、完善的网络行为管理解决方案。

为满足客户的不同需求，嵌入式安全网关产品对外提供嵌入式软件系统与嵌入式软硬一体化产品两种产品形态，其中软件系统提供给部分客户与其已有硬件相适配，软硬一体化产品为软件加硬件搭配的一体化安全网关产品。两种产品形态相辅相成，为客户提供全面、灵活的产品形式。

经过多年的发展，ABT SPOS 系统提供的嵌入式安全网关平台、模块、引擎、算法、特征库等技术已服务了业界众多知名厂商，如华为、新华三、星网锐捷、迈普通信、卫士通、启明星辰、360 网神、任子行、绿盟科技等大型企业。基于 ABT SPOS 系统的支撑，厂商可加速推出各类安全网关产品，同时也可以将应用层安全能力融入现有网络设备和通信设备中作为增强。这些安全产品和安全特性最终服务于国内各大行业与企事业单位的部分网络中，包括国家电子政务网、多个部委专用网络、各大运营商网络、大型金融机构网络、国家电网与能源网络、大型高校网络、大型医院网络等各种场景。

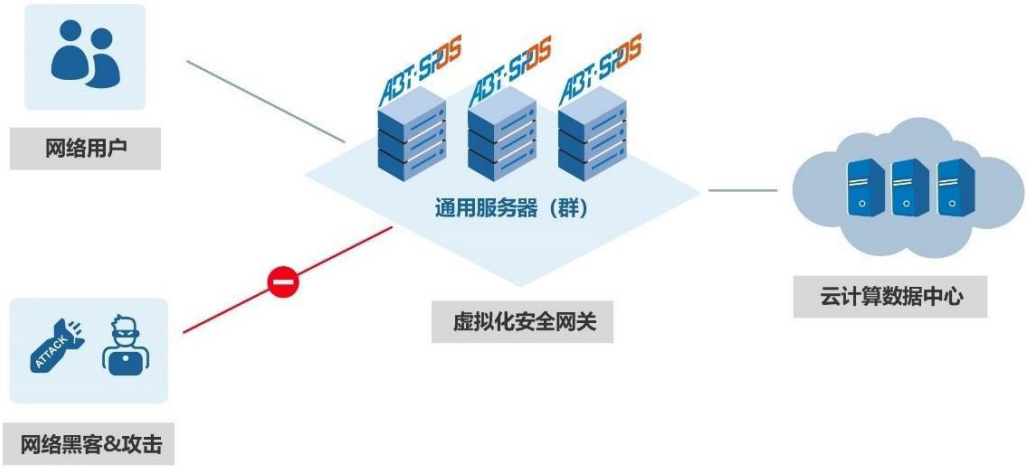
2) 虚拟化安全网关

随着云计算和虚拟化技术在数据中心建设方向的应用，数据中心基础架构从传统的集成数据中心向虚拟化数据中心转型。虚拟化数据中心安全防护的核心是网络安全防护的虚拟化，通过虚拟化技术将网络安全防护与服务器、网络设备等硬件环境进行深度适配，以高速自动化的方式分配与重新配置，使用户可以轻松地通过软件化的方式实现安全资源自由调配。

安博通虚拟化安全网关是基于 ABT SPOS 网络安全系统平台，通过虚拟化技术将安全防护特性与虚拟计算、虚拟存储、虚拟网络适配并融合到通用服务器中，形成标准化的防护单元，多个防护单元通过资源池方式汇聚成数据中心整体安全架构，并通过统一的管理平台实现可视化集中运维管理。

虚拟化安全网关主要应用场景如下图所示：

图 7 虚拟化安全网关的主要应用场景



资料来源：公司招股说明书，东海证券研究所

虚拟化安全网关以通用服务器为硬件载体，主要应用于大型数据中心和云计算中心，以安全资源池的形式满足公有云、私有云、混合云等多种云场景下的安全需求，并通过统一的管理界面实现全网安全资源池的分配和调度，主要用户包括政务云数据中心、运营商数据中心、金融数据中心和公有云服务提供商等。

（2）安全管理产品

随着多层面的网络安全威胁和安全风险的不断扩大及演化，网络攻击行为向着分布式、大规模、复杂化、利益化等趋势方向发展，防火墙、防病毒、入侵检测、单向隔离、数据加密等多种单一的网络安全防护措施之间由于相互缺乏及时、有效的整体关联性，已不能满足网络安全防护和安全管理的迫切需求。

特别是随着 SDN、虚拟化、分布式计算等技术的逐渐成熟，云计算平台应用和部署的越来越广泛，如何构建和管理安全可靠的云计算环境成为当前服务提供商业务开展的掣肘之一，需要积极开展从被动防御向主动防御转变的能力和体系建设以进一步提升网络及云计算平台的安全管理和运营水平。

基于大数据分析与可视化技术，公司在 ABT SPOS 网络安全系统平台之上打造了安全管理产品，主要包括流量可视化、策略可视化、云安全管理产品等。

针对新型的网络攻击手段与高级持续性威胁，通过采集网络中各类网关设备与监测设备产生的数据与流量，运用安全大数据分析、深度机器学习与流量可视化技术，发现并阻断网络中传统技术无法检测出的违规行为与未知威胁，这些产品已经成为构建网络安全态势感知系统的重要组成部分。

安全管理产品基于 ABT SPOS 网络安全系统平台开发，依据国家网信部门网络安全监测预警和信息通报制度的技术要求设计，部署在网络管理集中监控位置，通过大屏显示系统呈现和运维管理。该产品利用数据融合、数据挖掘、智能分析和可视化技术，直观显示网络环境的实时安全状况，对潜在的、恶意的网络攻击行为进行识别和预警，提升安全设备的整体效能，具备网络安全管理和预判能力，为网络安全提供运维保障，其工作流程如下图所示。

图 8 安全管理产品的工作流程

资料来源：公司招股说明书，东海证券研究所

公司提供的数据分析与运维平台等安全管理产品，通过集成到太极股份、中国电信系统集成等客户的整体解决方案中，已经应用于北京首都国际机场网络安全保障工程、新华通讯社全媒体供稿及电子商务平台、国家企业信用信息公示系统信息化工程主体部分、中国地震信息网络安全防护项目、全国人大信息中心电子政务外网等级保护建设项目等。

（3）安全网关产品与安全管理产品之间的关系

安全管理产品与安全网关产品不存在竞争关系，是互相协同关系。安全管理产品作为核心组件，面向整个网络的全局层面，管理和分析所有跨厂商安全设备节点；安全网关产品部署在具体的单个网络节点中，例如网络和安全域边界，负责该节点的安全防护。二者协同工作时，先通过安全管理产品分析宏观趋势，再通过安全网关产品处置具体存在问题的节点，形成综合解决方案。

在技术方面，安全网关产品的基础是处理网络通信流量的转发，在完成各类通信任务的基础上进行安全分析与防护，主体以网络流量为基础数据来源，以硬件无关化、多核并行操作系统为主要核心技术。

安全管理产品本身并不参与网络通信或流量转发，而是通过收集大量通信网络中重要节点的配置文件、安全策略、实时状态等信息进行计算和分析，主体以网络节点信息为基础数据来源，以网络行为画像和隐秘通信挖掘、安全策略配置数据挖掘与分析、安全合规路径可视化分析、安全资源的统一管理和部署为主要核心技术。

（4）各类产品及业务的产品形态

公司对外销售安全网关产品和安全管理产品，可以根据客户的需求，以软件或软硬件一体化整机形态销售，而网络安全服务主要是提供安全技术开发服务和安全运维服务。

表 2 各类业务产品形态

业务分类		产品与服务名称	产品形态
网络安全产品	安全网关产品	嵌入式安全网关	以软件或软硬件一体化形态销售
		虚拟化安全网关	以软硬件一体化形态销售
	安全管理产品	安全管理产品	以软件或软硬件一体化形态销售
网络安全服务			安全技术开发服务与安全运维服务

资料来源：招股说明书，东海证券研究所

1.3.2. 网络安全服务

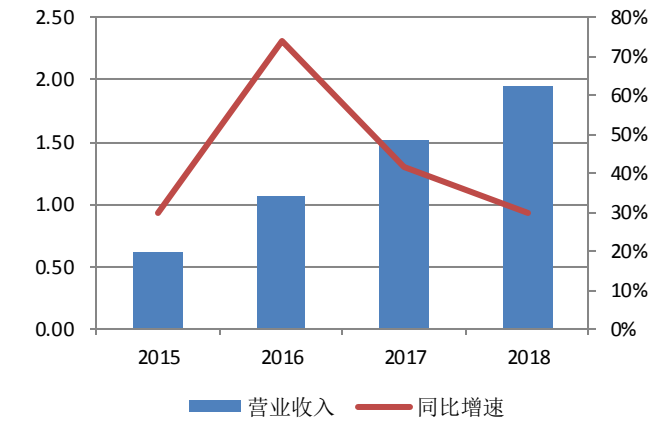
目前，公司网络安全服务主要为安全产品技术开发与安全运维服务，根据客户的个性化需求，在公司主营产品基础上定制开发扩展功能或个性化功能，或按照定制化需求开发产品特性或提供解决方案，同时提供产品运维保障服务。

报告期内，网络安全服务在营业收入中所占比重较小，主要为了满足部分客户的多样化需求，能够对公司业务发展起到一定的补充作用。

1.4.公司营收和净利润保持较快增长

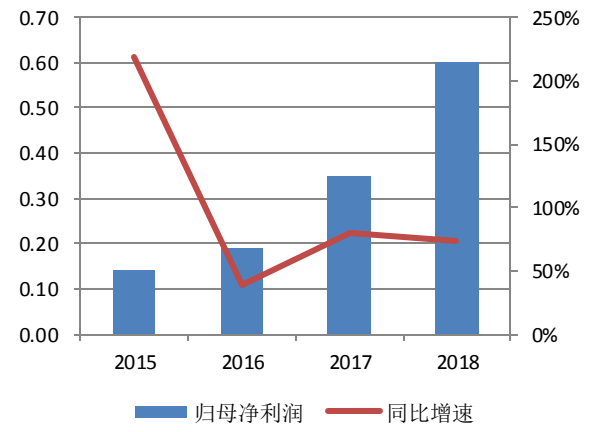
公司营业收入和净利润增速较快。2016-2018 年，公司营收分别为 1.06 亿元，1.51 亿元和 1.95 亿元，2016 年到 2018 年的增速分别为 73.87%，41.77%和 29.58%；归属母公司股东的净利润分别为 0.19 亿元， 0.35 亿元和 0.60 亿元，2016 年到 2018 年的增速分别为 39.47%，80.13%和 73.51%。

图 9 公司营业收入（单位：亿元，%）



资料来源：Wind，东海证券研究所

图 10 公司归母净利润（单位：亿元，%）

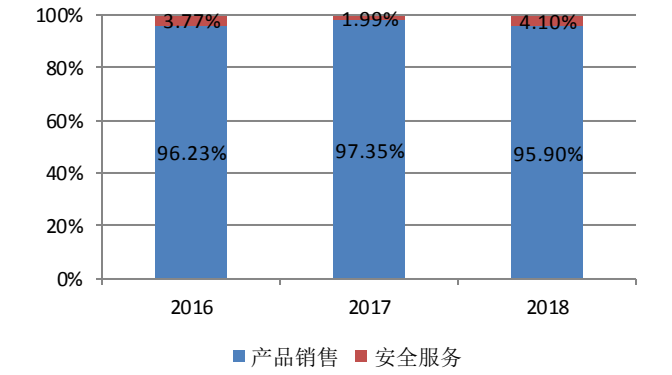


资料来源：Wind，东海证券研究所

1.5.公司净利率提升较快

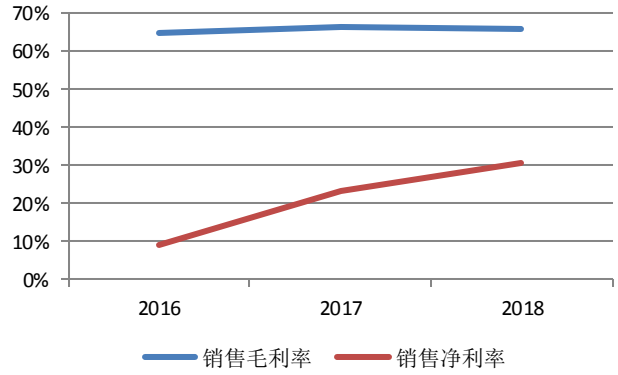
公司主营业务以网络安全产品销售为主，近年来，公司业务构成基本稳定。2016-2018 年，网络信息安全产品销售占公司总营收的比例分别为 96.23%，97.35%，95.90%。公司近三年综合毛利率维持在 65%左右。2016-2018 年，公司主营业务综合毛利率分别为 64.60%，66.15%和 65.88%，毛利率水平较高。公司三年销售净利率分别为 9.19%，23.46%和 30.63%，净利率水平逐步提升。

图 11 公司各产品营收占比



资料来源：Wind，东海证券研究所

图 12 公司销售毛利率和销售净利率



资料来源：Wind，东海证券研究所

2.行业情况分析

公司主营业务为网络安全核心软件产品的研究、开发、销售以及相关技术服务。根据国家统计局发布的《战略性新兴产业分类（2018）》，公司所处行业为“网络与信息安全软件开发”；根据中国证监会公布的《上市公司行业分类指引》（2012 年修订），公司所处行业为“I65 软件和信息技术服务业”；根据国家统计局发布的《国民经济行业分类》（GB/T4754-2017），公司所处行业为“软件和信息技术服务业”。根据公司主营业务的服务领域，公司属于网络安全行业。

2.1.网络安全行业发展状况

2.1.1.IPv6 应用前景广阔，安全问题亟待解决

网络互连协议（IP）作为全球互联网的基础协议，在过去二十多年中支撑了 Internet 的飞速发展，但是 20 世纪 80 年代初设计的 IPv4 协议没有能预测到互联网的爆炸性增长，2011 年最后一批 IPv4 地址分配完毕，全球已经进入 IPv4 地址资源枯竭的时代，但物联网的发展要求使用更多数量级的 IP 地址。IPv6 协议作为下一代协议，被设计用以提供更多的 IP 地址 。

根据第 43 次《中国互联网络发展状况统计报告》显示，截至 2018 年 12 月，我国 IPv6 地址数量为 41,079 块/32，年增长率为 75.3%，域名总数为 3,792.8 万个，其中“.CN”域名总数为 2,124.3 万个，占域名总数的 56.0%。我国正在持续推动 IPv6 大规模部署，数据显示，截至 2018 年 12 月，IPv6 地址数量较 2017 年底增长 75.3%。

在 IPv6 飞速发展的同时，针对 IPv6 的安全措施却有所滞后，现在 IPv6 持续面临协议自身安全、关联协议安全和过渡技术安全等多种安全问题，传统安全产品功能在 IPv6 协议上的应用也往往存在问题，亟需得到解决。山石网科在其 2018 年 8 月发布的 Stone OS5.5R6 版本中实现了下一代防火墙功能全面支持 IPv6。360 企业安全集团也在此方向上进行重点投入，2019 年与清华大学成立联合研究中心，重点研究以 IPv6 协议为标志特征的下一代互联网安全体系，包括 IPv6 环境下的真实源地址验证技术、访问控制与防火墙技术、IPv6 网络地址空间中的资产发现与安全漏洞扫描、入侵检测与异常检测、拒绝服务攻击检测等。

2.1.2.信息安全产品国产化自主可控趋势日益显著

2017 年 7 月，国家互联网信息办公室起草《关键信息基础设施安全保护条例（征求意见稿）》，提出顶层设计、整体防护、统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。

信息安全产业作为信息安全技术、产品和服务提供者和实施者，承担着国家信息安全防御和保障的历史使命，发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

近年来，国内信息安全厂商快速发展，依托本地布局的产品和研发团队，对用户需求理解更为透彻，对新需求的响应更为迅速，产品性价比更高，部分功能特性已超过国外厂商，但在高端产品市场的竞争力仍相对较弱。“十三五”时期，我国将大力实施网络强国战略，要求网络与信息安全有足够的保障手段和能力，通过切实推进自主可控和国产化替代，政策化培养和市场化发展双向结合，信息安全市场国产化脚步逐步加快。拥有自主可控的标准、技术、产品的信息安全厂商，将在为政府、行业服务的大背景下，充分应用包括云计算、大数据等技术，把握产业发展机遇，不断扩大市场份额，实现对国外信息安全产品的战略性替代，在核心应用领域和国内产业转型升级的变革中发挥重要作用，在国家网络信息安全领域中担当核心角色。

从业界观察，2018 年 12 月 5 日，启明星辰与天津飞腾信息技术有限公司签署战略合作协议。启明星辰全资子公司网御星云发布高性能自主可控网关型产品，它的核心处理器、操作系统、网络处理器、内存等均实现了自主化；天融信于 2010 年启动国产 CPU 芯片应用研究，并于 2013 年至 2015 年先后发布龙芯系列与兆芯系列防火墙、入侵检测等安全硬件产品。

2.1.3.云安全、物联网安全、工业互联网安全等市场将迎来爆发机遇

根据赛迪顾问股份有限公司发布的《2019 中国网络安全发展白皮书》，2018 年，中国云安全市场规模达到 37.8 亿元，增长率为 44.8%。公有云的多租户共享场景将导致可信边界的弱化，威胁的增加，因此构建基于云的纵深防护体系成为应对公有云安全威胁的重要手段。私有云、行业云领域，众多厂商积极在云安全资源池、云工作负载保护平台等重点领域加速布局，公有云领域，公有云安全防护发展态势持续向好，领域生态初步成型。

图 13　中国云安全市场规模

资料来源：公司招股说明书，东海证券研究所

在“互联网+”时代，物联网发展迅猛，正加速渗透到生产、消费、安防和社会管理等各领域，物联网设备规模呈现爆发性增长趋势，万物互联时代正在到来。物联网给我们的工作和生活带来便捷的同时，也带来了风险。物联网安全事件从国家、社会、个人层出不穷，物联网设备、网络、应用面临严峻的安全挑战。

物联网安全将成为万亿规模市场下的蓝海“潜力股”，2018 年中国物联网安全市场规模达到 88.2 亿元，增速达到 34.7%。

图 14 中国物联网安全市场规模

资料来源：公司招股说明书，东海证券研究所

物联网安全防护是要实现物联网的感知层、网络层及应用层的安全问题。应用层要实现大数据安全以及对已有的安全能力的集成，网络层要解决网络传输、基础设施以及边界安全等问题，感知层涉及大量终端，一方面是在终端设备生产环节加入安全芯片和防护措施，另一方面要增加物联网安全网关，实现对终端的安全防护。

由于工业互联网推动企业信息科技（IT）和操作技术（OT）融合，因此工业互联网安全是工业生产安全和网络空间安全相融合的领域，包含了工业数字化、网络化、智能化运行过程中的各个要素和环节的安全，主要体现为工业控制系统安全、工业网络安全、工业大数据安全、工业云安全、工业电子商务安全、工业 APP 安全等。

2018 年，对制造、通信、能源、市政设施等关键基础领域的攻击事件频频发生，受到攻击的行业领域不断扩大，造成后果也愈加严重，工业互联网安全的市场关注度随之提升。随着智能制造和工业互联网推进政策的不断出台，政府及企业开始逐步重视对工业互联网安全的投入，工业互联网市场具有较快的增长率。

据赛迪顾问发布的《2019 中国网络安全发展白皮书》，2018 年中国工业互联网安全市场规模达到 94.6 亿元。

图 15 中国工业互联网安全市场规模

资料来源：公司招股说明书，东海证券研究所

2.1.4.威胁情报市场平稳起步

在工信部印发的《公共互联网网络安全威胁监测与处置办法》中提到，为深入贯彻习近平总书记关于网络安全的重要讲话精神，积极应对严峻复杂的网络安全形势，进一步健全公共互联网网络安全威胁监测与处置机制，维护公民、法人和其他组织的合法权益，要求工信部和各省、自治区、直辖市通信管理局及时发现和处置被用于实施网络攻击的恶意 IP 地址、域名、URL、电子信息、程序、安全隐患以及其他的安全事件和隐患情形。面对上述问题，威胁情报是一个很好的解决方案，其可以类比为存在于互联网上的一个关于威胁信息的开放数据库，对外提供查询检索服务。

根据中国信息通信院发布的《2018 年度中国网络安全产业白皮书》，2015 年以来，我国的威胁情报市场逐步发展，表现在：一是龙头企业建立威胁情报中心，提升自身安全能力，例如 360 威胁情报中心，依托云端大数据技术自动化处理和人工运营配合，提供多种类型的威胁情报服务；绿盟威胁情报中心（NTI），利用多源情报清洗与归并技术、大数据关联分析技术等关键技术实现情报自动化处理，助力构建立体协同防御生态。二是专注于威胁情报领域的创新企业逐渐涌现，例如，微步在线（ThreatBook）相继推出了威胁情报搜索引擎、情报社区、以及在线新建威胁检测平台、威胁情报分析和管理平台等产品和服务；天际友盟借助本地安全情报中心（SIC）实现与客户本地、云端平台对接，提供多源情报和管理服务。三是产业联盟等搭建威胁信息共享平台，中国互联网网络安全威胁治理联盟汇聚国内 90 余家企业，强化互联网网络安全威胁情报共享和协作，天际友盟、思睿嘉得（北京）信息技术有限公司等企业发起成立烽火台安全威胁情报联盟，通过天际友盟 RedQueen 平台，实现威胁情报的交互。2018 年，威胁情报的应用进入了成熟期，其核心作用主要包括判断 IP 地址、URL 域名、文件 HASH 签名、DNS 服务器等关键网络元素的威胁信誉和具体信息，与各类防御体系进行整合提供威胁防御服务。

2.2.网络安全行业创新领域未来发展趋势

2.2.1.自主可控技术发展保卫国家网络空间

“十三五”时期，信息安全市场的自主可控和国产化替代趋势非常明确。在技术方面，网络安全产品为了完成自主可控，必须在以下关键组成部分实现国产化替代，包括：芯片、操作系统、数据库和中间件。

从芯片角度分析，国内的龙芯、申威、飞腾和兆芯，分别使用 MIPS、Alpha、ARM 和 X86 架构，不论是自主研发指令集和微结构，或是购买外厂商指令集授权配合自主研发的微结构并开放源码检查，都可以满足现阶段安全可控的要求。对于桌面级、服务器级、高性能计算和超级计算的各种场景，目前国产芯片都已经基本完成了覆盖，在相关的对比中，性能上相比 Intel 已经拉近差距甚至达到相媲美的水准，在普通办公和通信场景下，国产芯片已经达到了应用标准。

从国产操作系统方面分析，中标麒麟、普华等国产操作系统，可以满足自主可控需求，也已经形成面向桌面操作系统、服务器操作系统、安全操作系统等多类型产品，能支持 X86、龙芯、申威、飞腾等 CPU 平台。国产操作系统生态发展逐渐成熟，基本可以实现文档处理、影音播放、网络接入等业务需求，对于嵌入式通信产品也提供很好的支持，具备了使用条件。

类似地，在国产数据库和中间件领域，武汉达梦数据库有限公司、北京东方通科技股份有限公司等厂商的产品长期耕耘国产市场，其产品水准虽然距离国际领先依然存在差距，但都可以满足常用的应用场景。

综合以上情况分析，对于自主可控技术的关键组成部分，业界已经基本具备了国产化替代国外产品的能力，应用条件已经相对成熟。可以预见的是，自主可控产品将在这样良好的条件下大力发展，真正做到保卫国家网络空间。

2.2.2.物联网安全迎来发展机遇

根据腾讯发布的《2018 年 IoT 安全威胁分析报告》显示，2018 年 IoT 设备增长迅猛，全球的设备数量已经达到 70 亿台，如果保持每年 20%左右的增长速度，预计 2020 年将达到 99 亿台。在所有 IoT 设备中，路由器、摄像头和智能电视是被攻击频率最高的三款 IoT 设备，占比分别达到 45.47%、20.71%和 7.61%。

由于拥有 IoT 设备数量众多，且很多设备存在漏洞和弱口令，相互攻击感染问题严重，导致我国成为全球 IoT 攻击最频发的国家，同时也是最大的受害国（占总攻击的比例达到 19.73%）。

在 5G 及 IoT 领域，终端数量极其庞大，当大量的终端设备遭到入侵控制后，攻击者可以利用这些设备进行 DDoS 攻击或进行恶意挖矿，造成物联网设备上的正常业务受到影响。更严重的是，这些遭受入侵的物联网设备还会在暗网上被挂出，出租 DDoSaaS（DDoSasaService）服务，被当作跳板进行更多攻击，给组织和个人带来大量损失。

从共性上分析，IoT 安全有以下几个方向，分别是：软件版本安全、终端类型准入、流量访问控制、安全威胁检测、调度平台对接等。IoT 的各个方向已经发展成较为独立的领域，在各个领域上安全需求有所区别。随着未来 5G 及 IoT 物联网领域的发展，其将为未来 IoT 安全市场带来巨大的空间。

2.2.3.云情报、机器学习等人工智能预测技术成为安全防护的重点

传统的安全架构中，较多依赖特征匹配的模式。在这种模式中，防护设备需要先将某个攻击事件写入特征库，然后才能防御这个攻击，而且安全设备的特征库，数量是非常有

限的，所以最大的问题在于滞后性和局限性，防护方永远落后于攻击方，对 0day 等未知威胁无能为力。

如今，网络安全界的潮流是让安全变得更主动、更前置，主要的技术手段包括云威胁情报和机器学习预测技术。

云威胁情报方面，在云平台上存储的特征数量达到数亿乃至数十亿数量级，安全产品接入云威胁情报后，其理论的特征范围从本地扩大到整个云情报库，威胁情报的更新频率非常迅速，可以弥补容量短板，解决未知威胁问题；出现突发安全事件时，情报平台可紧急推送消息到流量安全产品，联动完成自动紧急防护，解决滞后性问题。

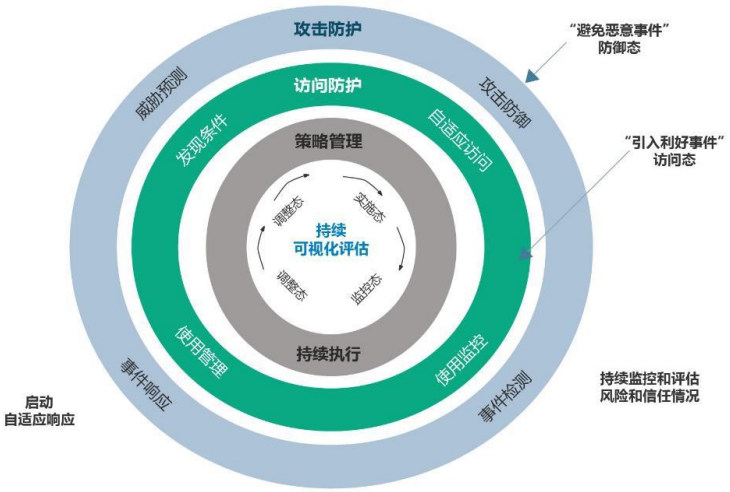
机器学习预测方面，安全产品可以发现和存储海量的安全事件，但安全防护不能永远是被动的，而是应该通过分析过去一段时间的事件，通过机器学习技术分析规律，从而对未来一段时间内可能发生的安全威胁进行预测，以便提早进行针对性防护措施。在网络安全领域，已经有产品应用贝叶斯算法、Bayesian-MCMC 等知名的预测算法进行安全事件预测，当机器学习技术更加成熟，网络安全的预测将会变得更加高效准确。

2017 年，国内数据库安全审计与防护产品市场依旧竞争较为激烈，公司在政策和自身品牌的影响下逐步发力，占据 7.2%的市场份额，仅次于启明星辰的 10.2%，排名第二。以数据库技术和影响力领先的国际厂商 IBM、Imperva，以 6.9%与 6.4%的市场份额排名第三及第四。

2.2.4. 自适应安全架构促使智能安全落地

2014 年，Gartner 针对高级攻击首次提出了自适应安全架构的理论框架 V1.0 版本，将防御体系的流程定义为循环的预测、防御、监控和响应四个阶段，并指明了各个阶段的主要动作。随后，在 2017 年和 2018 年，自适应安全架构相继发布了 V2.0 和 V3.0 版本，以便不断适应网络安全技术的发展和补充遗漏之处，下图为自适应安全架构 V3.0 图示。

图 16　自适应安全架构



资料来源：公司招股说明书，东海证券研究所

继2016年自适应安全架构被广泛认可之后，很多安全产品都在按照此架构进行演进，也有很多产品和解决方案遵循“事前-事中-事后”、“DetectandResponse”等架构流程，

也基本是出自于自适应安全架构。自适应安全理论体系打破了传统安全的理念，在安全架构中增加了诸多环节，指明了不同环节之间的融合关系，这促使了安全产品不仅要不断推出新功能，还要将不同的功能进行互相关联和顺序编排，从而推进了智能化技术在安全产品上落地。在未来，自适应安全将会纳入更多环节，安全产品的特性也将会越来越多，智能化发展趋势已成必然。

2.2.5.多维度的安全分析和可视化呈现

在安全产品的发展过程中，将检测到的关键信息以日志等方式留存下来，以便满足检索和合规要求，这种技术架构存在了很长时间，但并未产生足够的价值。

如今，安全事件变得越来越多样化，APT 攻击常常由身份盗取、系统入侵、数据回传等多个环节构成，涉及到安全防护的多个环节，传统的单一层面安全分析无法解决问题。

在 IDC 发布的《中国安全管理平台（SOC）市场份额》中提出，在企业频频遭受多样化攻击的今天，恶意威胁的集中化、可视化和可分析化渐渐成为企业对安全投资的趋势。未来的安全管理分析，一定是基于多个维度综合进行的，方案需要覆盖到网络安全的主要板块例如边界安全、主机安全、流量安全等等方面，站在防御体系的宏观角度提供给用户统一的分析工具。另外，场景化数据分析方案已经流行开来，将采集到的数据按照不同的场景，例如潜在的泄密手段、舆论风险、员工离职倾向等，进行针对性的分析与呈现，让安全与用户的业务结合更紧密，从而体现出价值，而不仅仅是一种投资。

2.2.6.云安全催生虚拟化安全新架构

云安全技术的发展，不仅更好地解决了云内安全问题，也让以 NFV（网络功能虚拟化）的生态得到了良好的发展。目前，以安全能力虚拟化＋安全能力调度为技术架构的众多一体机产品，例如等级保护一体机、网点出口一体机、数据中心安全防护一体机，已经实现了对嵌入式网络通信平台的部分替代。

在安全功能要求复杂且灵活，而性能要求不高的场景中，传统安全解决方案存在较大的缺陷，如果使用盒子类产品，不仅需要配置几种甚至十几种产品，而且无法做到根据不同用户群和不同业务执行不同的调度策略，运维和采购成本都非常高。而使用安全虚拟+能力调度的方法，所有安全能力软件化部署，可以灵活地按需配置几十种性能符合要求的能力，还能按需灵活地调整编排，按照软件定义安全的理念，以低成本、高灵活度、简单运维的优势满足业务需求。

未来，网络安全技术的划分会更加精细，安全能力将会越来越多，尤其是在私有云等环境下尤为明显，虚拟化安全新架构将会有更广阔的应用前景。

3.公司看点

3.1.领先的技术研发优势

3.1.1.研发团队优势

经过多年的技术研发和业务经验的积累，公司形成一支拥有丰富经验的安全核心技术专业团队，具有较强的团队研发和技术攻坚能力，能够满足客户的场景需求，提供专业化的产品和服务。

截至 2018 年 12 月末，公司拥有研发人员 87 名，技术支持人员 32 名，研发人员及技术支持人员合计占员工总人数的比例为 64.67%，覆盖产品研发、算法研究、攻防研究、

病毒木马研究、漏洞研究、安全服务化等领域。公司在北京、武汉设立了技术与产品研发中心，在天津设立了网络攻防研究实验室，持续的研发投入为公司研发创新能力的构建、核心技术的形成提供了有力支撑与保障。

3.1.2.技术积累优势

通过持续的技术创新，截至本招股说明书签署日，公司已申请发明专利共 109 项，其中 12 项已取得发明专利证书，拥有计算机软件著作权 74 项，已形成了具有自主知识产权的核心技术和知识产权体系。报告期内，公司研发投入分别为 1,585.22 万元、2,652.84 万元和 2,655.37 万元，占同期营业收入的比例分别为 14.91%、17.60%和 13.59%。

安全策略配置突破核心技术算法。

传统的安全管理产品将安全设备硬件作为管理对象，存在较大的局限性，原因在于对网络安全起到作用的是安全设备上运行的安全策略。安博通安全管理产品通过计算网络安全策略访问路径，可以计算出整网业务的真正交互地图，配合正确的业务安全基线，帮助用户计算最准确的业务访问路径，并且能够伴随着策略的变化而完成自动化变更和实时告警。

2015 年，公司实现了安全策略路径相关核心算法的突破，通过不断地优化，在 2017 年将 10000 节点规模大型网络的策略路径计算时间控制在 5-10 分钟，达到了国外竞争对手同等级水平；同时，公司投入研发大数据算法方向，将安全资产、恶意行为、流量威胁和策略路径四类数据进行综合分析，进行关键参数的不断调整和验证，给出了整网暴露攻击面的较准确的算法，在国内尚未有竞争对手实现同类方案。

依托于策略路径和攻击面分析两项核心技术算法的突破，公司在国内率先推出了 4D 攻击面可视化产品和解决方案，为包括金融行业、电信运营商、军队等核心行业提供具有自有知识产权的产品和解决方案，使之在该方向上避免了只能选用国外产品或解决方案的现状，规避了网络核心信息泄露的风险。公司相关产品及解决方案进入成熟稳定阶段，该方案形成的产品已连续两年入选工信部“网络安全试点示范项目”，2019 年入选工信部网络安全技术应用试点示范项目。

硬件无关化技术方向实现自主可控。

在网络安全行业，不同的硬件体系架构体现的技术优势存在差异性，例如在计算能力、通信表现、图形化展现等方面表现不同，业内厂商一般采用软硬件紧耦合的技术路线，仅支持 1-2 种体系架构，而且在不同体系架构间代码重构量偏大，无法快速切换。

厂商客户根据自身实际技术情况，对安全网关产品适配在不同体系的硬件平台上存在需求。2013 年，公司投入研发对安全网关产品进行硬件无关化技术升级，使用用户态和硬件松耦合的技术路线，将与体系架构相关的代码进行封装，从而实现软件在不同体系架构上的代码高度一致性，降低了体系架构间切换所需的代码重构量。凭借硬件无关化技术，安全网关产品已经在 MIPS 多核、x86、ARM 以及国产的龙芯、申威、飞腾 6 种架构的数十款硬件上实现产品化，同时也在 KVM、VMware、Xen3 种主流虚拟化平台上实现产品化。

在国产自主可控产品方面，不同的厂商客户跟随了不同的硬件体系路线，公司将安全网关产品以软件形态部署在龙芯、申威、飞腾三种不同的体系架构中，推出了满足自主可控要求的国产防火墙、网络安全审计和入侵防御产品。

安全网关产品功能丰富。

公司安全网关产品的功能丰富，涵盖了应用账户（App-ID）、用户账户（User-ID）、内容账户（Content-ID）三个网络安全流量分析的主要技术方向，提供超过 5000 种的主流互联网应用识别库、1000 万条以上的网址库以及超过 7000 万条以上的威胁情报库，能够帮助用户发现和管控隐藏在高层应用中的恶意内容。公司在获取华为、启明星辰、新华三、安恒信息等行业内知名客户的过程中，多次参加由客户公开组织的技术测试，考察产品功能、性能、稳定性、安全性等的综合表现。尽管测试的标准根据客户需求存在差异，但公司安全网关产品均排名领先。公司对安全网关产品根据技术演进和市场情况持续更新迭代，在长期合作过程中，客户针对更新版本的安全网关产品进行持续性测试，公司安全网关产品功能及稳定性能够持续满足客户的需求。

3.2.优质的客户基础

公司凭借领先理念、创新能力及技术服务能力，紧贴客户业务场景提供高质量产品和专业化服务，赢得了客户的信赖。经过多年发展，公司积累了一大批行业内知名客户，包括华为、新华三、星网锐捷、卫士通、启明星辰、360 网神、任子行、绿盟科技、太极股份、荣之联、中国电信系统集成、迈普通信等知名产品与解决方案厂商。这些知名客户在行业内的地位为公司产品的开发、技术的创新及解决方案的完善提供了动力。在此基础上，公司对主要客户的需求深入分析和总结，将实践经验应用于其他行业，为客户提供更为全面优质的服务。

3.3.快速的上游技术响应和服务

作为业内的上游技术输出厂商，公司产品在客户处面临着各种各样的差异化应用场景，需要跟客户的自有产品进行深度融合对接，这对公司的技术响应和服务提出了较高的要求。公司设置专业的售前售后技术服务部门，团队深入客户业务场景了解和传递需求，为用户提供技术指导和支撑，产品和研发部门快速响应需求，使得产品快速迭代创新，支撑客户快速多变的业务发展。

3.4.良好的工程师文化氛围

良好的企业文化是公司可持续发展的保障。公司以打造“可视化网络安全技术引领者”为愿景，以“持续创造极简并极致的网络与安全业务价值新体验”为使命，公司内部始终强调“勇敢、奋斗、开放、创新”核心价值观。公司信奉忠于职守、尽心尽责的责任感；同时以专业精神、专业技能、专业流程、专业品质，向客户提供高质量的产品与服务；公司内部强调依靠团队精神来实现理想，分享知识和快乐；通过持续创新满足客户日益变化的安全需求。

4.募集资金用途

公司拟向社会公开发行不超过 1,279.50 万股，占发行后总股本的比例不低于 25%。发行后总股本不超过 5,118.00 万股。公司本次实际募集资金扣除发行费用后的净额将全部投资于以下项目：深度网络安全嵌入系统升级与其虚拟资源池化项目，安全可视化与态势感知平台研发及产业化项目和安全应用研发中心与攻防实验室建设项目。

表 3　募投项目及投资金额

募投项目名称	项目总投资	拟投入募集资金	建设周期
深度网络安全嵌入系统升级与其虚拟资源池化项目	15,800.00	15,800.00	36 个月

安全可视化与态势感知平台研发及产业化项目	7,663.00	7,663.00	24个月
安全应用研发中心与攻防实验室建设项目	6,311.00	6,311.00	24个月
合计	**29,774.00**	**29,774.00**	

资料来源：招股说明书，东海证券研究所

5.盈利预测

5.1.对比公司

A股上市公司中，与安恒信息业务类似的公司主要有启明星辰，绿盟科技，深信服，迪普科技，任子行等公司。

表4 可比公司

	毛利率	销售费用率	管理费用率	研发费用占营收比重	市盈率（TTM）
启明星辰	65.47%	24.30%	6.25%	21.19%	47.50
绿盟科技	76.93%	37.79%	10.66%	20.14%	65.70
深信服	73.32%	36.32%	4.03%	24.16%	75.60
迪普科技	70.70%	26.25%	3.33%	22.43%	76.50
任子行	51.15%	18.79%	10.24%	14.01%	34.30
平均值	67.51%	28.69%	6.90%	20.39%	59.92
安博通	65.88%	10.51%	9.15%	13.59%	

资料来源：Wind，招股说明书，东海证券研究所

5.2.盈利预测

根据行业的空间和公司的主要优点，预计公司2019-2021年总体收入分别为2.51、3.12和3.86亿元，同比增速为28.03%、24.81%和23.55%；归母净利分别为0.71、0.90和1.15亿元，同比分别增长15.76%、36.80%、30.59%。以发行后总股本0.512亿股计算，2019-2021年EPS分别为1.39、1.77和2.25元。参考对比公司启明星辰和绿盟科技最近的PE（TTM）值，我们建议以2019年对应EPS的30-40倍左右PE申购，申购价格大概为41.75-55.66元/股。

6.风险提示

产品集中风险，应收账款风险。

附录：三大报表预测值

资产负债表

单位：百万元	2018	2019E	2020E	2021E
货币资金	82.27	92.36	110.01	150.74
应收和预付款项	150.36	184.46	233.81	283.14
存货	14.32	21.29	25.17	33.14
其他流动资产	0.70	0.70	0.70	0.70
长期股权投资	0.00	0.00	0.00	0.00
投资性房地产	0.00	0.00	0.00	0.00
固定资产和在建工程	31.14	25.59	20.04	14.48
无形资产和开发支出	7.72	7.03	6.35	5.66
其他非流动资产	0.00	0.00	0.00	0.00
资产总计	286.52	331.44	396.08	487.87
短期借款	15.00	0.00	0.00	0.00
应付和预收款项	14.36	24.26	25.43	36.39
长期借款	0.00	0.00	0.00	0.00
其他负债	0.00	0.00	0.00	0.00
负债合计	29.36	24.26	25.43	36.39
股本	38.39	38.39	38.39	38.39
资本公积	117.55	117.55	117.55	117.55
留存收益	99.48	152.13	218.95	304.05
归属母公司股东权益	255.42	308.07	374.89	459.98
少数股东权益	1.75	-0.89	-4.24	-8.50
股东权益合计	257.16	307.17	370.65	451.48
负债和股东权益合计	286.52	331.44	396.08	487.87

现金流量表

单位：百万元	2018	2019E	2020E	2021E
经营性现金净流量	18.07	39.46	36.32	65.19
投资性现金净流量	-21.13	2.66	2.66	2.66
筹资性现金净流量	-2.33	-32.03	-21.33	-27.13
现金流量净额	-5.39	10.09	17.65	40.72

利润表

单位：百万元	2018	2019E	2020E	2021E
营业收入	195.35	250.11	312.17	385.70
营业成本	66.65	88.67	115.69	145.22
营业税金及附加	2.42	3.10	3.87	4.78
营业费用	20.52	26.27	32.79	40.52
管理费用	21.23	27.19	33.93	41.92
财务费用	0.20	-1.53	-2.24	-2.89
资产减值损失	2.27	2.27	2.27	2.27
投资收益	0.00	0.00	0.00	0.00
公允价值变动损益	0.00	0.00	0.00	0.00
其他经营损益	-26.55	-26.55	-26.55	-26.55
营业利润	55.50	77.59	99.31	127.33
其他非经营损益	0.47	0.47	0.47	0.47
利润总额	55.97	78.05	99.78	127.80
所得税	6.41	9.44	12.70	16.91
净利润	49.56	68.61	87.07	110.89
少数股东损益	-1.91	-2.64	-3.35	-4.26
归属母公司股东净利	61.55	71.25	90.42	115.16

主要财务比率

	2018	2019E	2020E	2021E
收益率				
毛利率	65.88%	64.55%	62.94%	62.35%
三费/销售收入	21.47%	20.76%	20.66%	20.62%
EBIT/销售收入	28.73%	30.58%	31.23%	32.37%
EBITDA/销售收入	29.34%	32.17%	32.51%	33.40%
销售净利率	25.37%	27.43%	27.89%	28.75%
增长率				
销售收入增长率	29.58%	28.03%	24.81%	23.55%
EBIT 增长率	85.31%	36.28%	27.47%	28.07%
EBITDA 增长率	80.46%	40.37%	26.12%	26.97%
净利润增长率	79.71%	38.43%	26.91%	27.36%
总资产增长率	24.36%	15.68%	19.50%	23.18%
股东权益增长率	25.24%	20.61%	21.69%	22.70%
经营营运资本增长率	36.85%	20.73%	28.52%	19.84%
业绩和估值指标				
EBIT	56.13	76.49	97.50	124.87
EBITDA	57.32	80.46	101.47	128.84
NOPLAT	49.30	66.88	84.74	108.00
净利润	61.55	71.25	90.42	115.16
EPS	1.60	1.39	1.77	2.25
BPS	6.654	8.026	9.766	11.983

资料来源：WIND，东海证券研究所

分析师简介：

黄伯乐：武汉大学本科，中央财经大学金融学硕士，2014年加入东海证券，从事计算机行业研究

附注：

一、市场指数评级

看多——未来6个月内上证综指上升幅度达到或超过20%

看平——未来6个月内上证综指波动幅度在-20%—20%之间

看空——未来6个月内上证综指下跌幅度达到或超过20%

二、行业指数评级

超配——未来6个月内行业指数相对强于上证指数达到或超过10%

标配——未来6个月内行业指数相对上证指数在-10%—10%之间

低配——未来6个月内行业指数相对弱于上证指数达到或超过10%

三、公司股票评级

买入——未来6个月内股价相对强于上证指数达到或超过15%

增持——未来6个月内股价相对强于上证指数在5%—15%之间

中性——未来6个月内股价相对上证指数在-5%—5%之间

减持——未来6个月内股价相对弱于上证指数5%—15%之间

卖出——未来6个月内股价相对弱于上证指数达到或超过15%

四、风险提示

本报告所载的全部内容只提供给客户做参考之用，并不构成对客户的投资建议，并非作为买卖、认购证券或其它金融工具的邀请或保证，建议客户如有任何疑问应当咨询独立财务顾问并独自进行投资判断。

五、免责条款

六、资格说明

东海证券股份有限公司是经中国证监会核准的合法证券经营机构，已经具备证券投资咨询业务资格。我们欢迎社会监督并提醒广大投资者，参与证券相关活动应当审慎选择具有相当资质的证券经营机构，注意防范非法证券活动。

上海 东海证券研究所

地址：上海市浦东新区东方路1928号 东海证券大厦

网址：Http://www.longone.com.cn

电话：（8621）20333619

传真：（8621）50585608

邮编：200215

北京 东海证券研究所

地址：北京市西三环北路87号国际财经中心D座15F

网址：Http://www.longone.com.cn

电话：（8610）66216231

传真：（8610）59707100

邮编：100089