中信建投证券 CHINA SECURITIES

证券研究报告·上市公司深度　　计算机应用

网络安全行业进入黄金发展期，龙头公司显著受益将加速增长

启明星辰（002439）

公司是国内网络安全领军企业，在包括党政军在内的多行业优势显著。公司拥有完全自主知识产权的 100 多款网络安全产品，多年来，启明星辰一直保持着我国入侵检测/入侵防御、统一威胁管理、安全管理平台、运维安全审计、数据审计与防护市场占有率第一位，已经成为政府、电信、金融、税务、能源、交通制造烟草、传媒等国内高端企业级客户的首选品牌。1996 年成立后公司经历了不同阶段的跨越式发展，从传统网络安全到建立“第三方独立安全运营”新模式，到不断推出基于云计算、大数据、物联网、工业互联网、关键信息基础设施保护、移动互联网等新场景的网络安全解决方案，提供覆盖全行业全技术的安全能力。公司能紧跟行业发展适时自研或者通过投资并购推出新产品、新业务，良好和完善体系化的营销体系优势、品牌优势和整体解决方案能力使公司成为多行业高端客户稳定合作伙伴。公司多年营业收入和净利润保持连续增长，财务表现稳健。自 2014 年至 2018 年，公司营收复合增长率 20.5%，扣非归母净利润从 1.26 亿元增长至 4.36 亿元，复合增长率 36%。

伴随行业政策、技术革新和新场景需求，2019~2021 年进入网络安全行业高景气周期，2019~2023 年行业复合增速超过 25%，行业龙头显著受益。“云大物移”新场景驱动下防护对象改变，企业网络边界逐渐消失，政府和企业网络安全防护理念发生较大变化，网络安全不再是“补丁”模式，而是与信息系统建设同时规划，促进信息安全占 IT 支出占比逐步从 2%提升至 5%以上。2019 年 5 月，《网络安全等级保护制度 2.0 标准》正式发布，实施时间为 2019 年 12 月 1 日，在新场景需求下等保 2.0 增加了新对象的安全防护如云计算平台、大数据平台、物联网系统、工业控制系统等，增加了对关键基础设施的防护如明确规定了轨道交通、电力能源等基础设施纳入保障范围，增加了对新产品和技术的要求，例如要实现态势感知，能够检测对重点节点及其入侵的行为，对各类安全事件进行识别报警和分析等等，**因此未来新产品、新行业和新的防护对象都将促进网络安全行业市场规模持续保持快速增长。**因此我们看到启明星辰作为龙头厂商，近年在轨交、医疗、工控安全、云安全等领域增长迅速。2019 年 HW 行动力度加大，由于 2019 年 HW 行动覆盖范围增加且考核排名机制趋严，对入侵检测、云安全、态势感知等产品带动作用明显。2019 年预计中国网络安全市场规模将达到 602 亿， IDC 预计 2018~2020 年中国网络安全市场年复合增速将超过 25%，网络安全行业迎来了发展的黄金年代。

伴随新应用场景出现和积极防御类网络安全产品快速增长，安全运营服务市场增长迅速，城市安全运营服务中心业务将促进公司

维持　　买入

石泽蕤

shizerui@csc.com.cn

18616092669

执业证书编号：S1440517030001

侯子超

houzichao@csc.com.cn

15216713023

执业证书编号：S1440518110003

发布日期： 2019 年 10 月 16 日

当前股价： 32.52 元

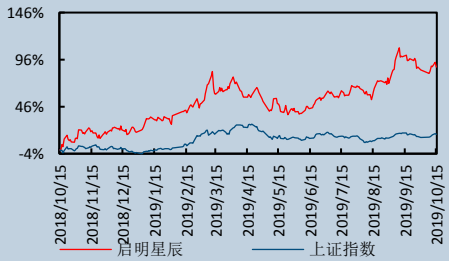
主要数据

股票价格绝对/相对市场表现（%）

1 个月	3 个月	12 个月
-5.47/-4.14	21.03/18.96	98.02/83.28

12 月最高/最低价（元）	36.27/16.86
总股本（万股）	89,669.26
流通 A 股（万股）	63,426.56
总市值（亿元）	291.6
流通市值（亿元）	206.26
近 3 月日均成交量（万）	991.39
主要股东	

股价表现



相关研究报告

19.08.07	【中信建投计算机应用】启明星辰(002439):行业多重利好驱动业绩高增长，投资并购生态优势逐步体现
19.04.29	【中信建投计算机应用】启明星辰(002439):现金流明显改善，行业高景气下收入提速

智慧城市大数据发展，为公司提供长期发展动力。未来三年，随着云计算、大数据与智慧城市的快速发展，更多的大型企业趋向于定制化安全服务，安全服务市场将持续增长，预计 2020 年安全服务市场规模将达到 108.6 亿元，未来三年复合增长率为 33.25%。未来城市安全运营中心一方面将为公司带来海量各领域安全数据，为公司积累城市安全大数据，促进公司长期的数据安全分析能力提升和产品研究能力提升；一方面城市运营中心也将增加公司与当地客户的粘性，通过发现当地客户基础设施和网络中存在的安全漏洞和问题，给客户提供更完善的解决方案，为公司带来安全解决方案或者安全产品订单。目前公司全国运营体系已基本形成北京、成都、广州、杭州四个运营业务支撑中心及二十余个城市级运营中心，未来在持续扩大已有运营中心业务的基础上，运营中心业务将向其他二三级城市拓展，目标 35 个运营中心。

2019~2020 年多重因素助力党政军行业网络安全需求加速增长，促进公司 2019~2020 年业绩加速。同时公司持续投资并购建设不断完善的网络安全生态，在网络安全技术快速迭代和创新中保持领导地位。受到军改影响，2018 年公司军工订单不达预期影响了公司 2018 年增速。而在十三五规划临近验收、军工行业订单重回高增长、等保 2.0 发布并实施、“云大物移”新场景对新产品和解决方案的需求加速行业发展、安可和自主可控需求增加等多重因素促进下，2019~2020 年预计各级政企单位有望加大网络安全投入和建设，服务于党政军和央企高端客户的行业龙头将显著受益，预计启明星辰 2019~2020 年业绩将和行业增速一样加速增长。在网络安全下游行业快速发展、新产品叠出的时代，网络安全公司生态体系建设的重要性。中国市场大型客户比较注重网络安全整体解决方案，要求承建网络安全项目的供应商具备整体规划能力和比较完善的产品体系。而随着云计算、物联网的快速发展，因此公司除了自主研发产品外，也通过投资并购能有效弥补整体解决方案的不足。近年公司一直通过并购和投资手段建设自己的网络安全生态，储备未来网络安全发展关键技术和巩固细分行业优势地位，有利于公司长期稳健发展。

投资建议：随着我国信息化程度提升，云大物移快速发展，国际局势紧张，国家对网络安全重视程度逐步提升，政策和需求共同驱动网络安全行业进入高景气周期，网络安全在 IT 开支占比也将逐步提升，2019~2023 年中国网络安全行业复合增速将达到 25%。2019 年行业迎来多重利好，军工订单恢复，安可进入正式实施阶段，促进公司营收和利润增速加速。作为国内网络安全领军企业，启明星辰走在智慧城市安全运营中心建设前沿，增强公司大数据能力和利用运营促进解决方案销售，安全服务获得快速增长。同时公司通过投资并购建立起的生态优势逐步体现，在新领域、新行业拓展速度较快，长期增长动力充足，我们预计 2019~2020 年公司归母净利润 6.59 亿元、8.31 亿元，给与“买入”评级。

风险提示：并购整合不达预期导致公司管理存在风险；网络安全行业高端人才竞争激烈导致公司自身创新发展放缓风险；行业内央企背景网络安全公司数量增加导致竞争加剧风险

表 1：启明星辰盈利预测表

	2017	2018	2019E	2020E	2021E
营业收入（百万元）	2,278.5	2,521.8	3,150.0	3,939.9	4,499.5
同比	18.2%	10.7%	24.9%	25.1%	14.2%
净利润（百万元）	451.9	569.0	658.6	831.3	958.0
同比	70.4%	25.9%	15.8%	26.2%	15.2%
EPS（元）	0.50	0.63	0.73	0.93	1.07
PE	64.53	51.25	44.28	35.08	30.44

资料来源：中信建投证券研究发展部，PE 对应 10 月 15 日收盘价

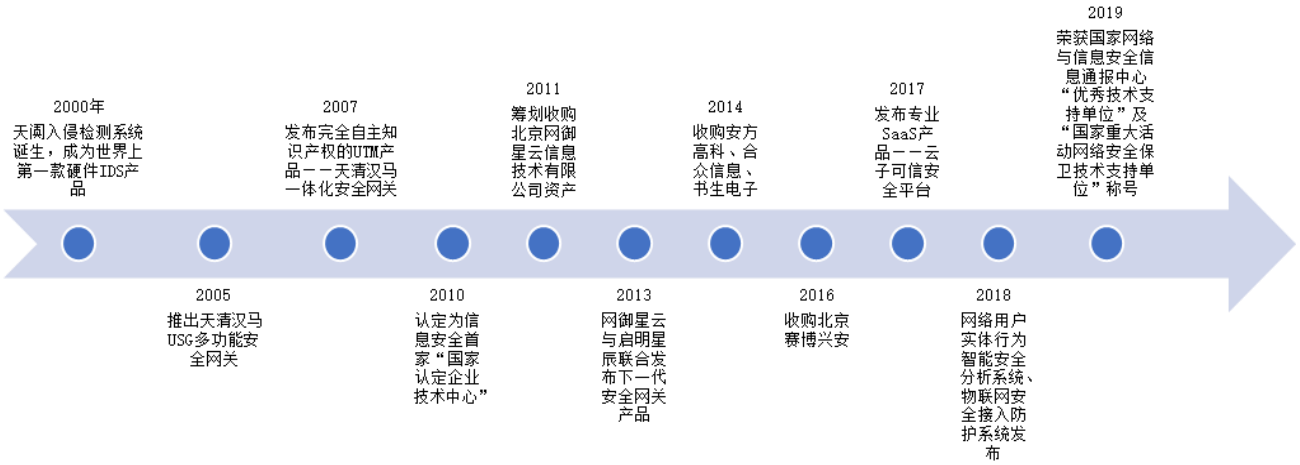
目录

图表目录

一、多行业高端客户认可的网络安全领军企业，解决方案全面、财务稳健

公司是国内网络安全领军企业，在包括党政军在内的多行业优势显著，提供覆盖多行业的完善解决方案。作为信息安全产业的领军企业，启明星辰一直保持着我国入侵检测/入侵防御、统一威胁管理、安全管理平台、运维安全审计、数据审计与防护市场占有率第一名。公司从 1996 年成立以后通过不断耕耘，已经成为政府、电信、金融、税务、能源、交通制造烟草、传媒等国内高端企业级客户的首选品牌。启明星辰自成立起，经历了不同阶段的跨越式发展，从传统网络安全到建立“第三方独立安全运营”新模式，到不断推出基于云计算、大数据、物联网、工业互联网、关键信息基础设施保护、移动互联网等新场景的网络安全解决方案，提供覆盖全行业全技术的安全能力，解决新技术带来的安全挑战，帮助城市全面提升安全能力。截至 2019 年中报，公司创始人王佳持有公司 27.03%的股份，是第一大控股股东，也是公司的实际控制人，公司第二大控股股东为严立先生，持有公司 5.29%的股份，与王佳女士为夫妻关系，一致行动人。

图表1： 启明星辰发展历程



资料来源：公司官网，中信建投研究发展部

公司产品覆盖广泛，产品线完善。启明星辰当前拥有完善专业的安全产品线，主要产品大类为安全网关、安全检测、数据安全与平台、 安全服务与工具、硬件及其他几大类，经营项目横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有 100 多产品型号，并根据客户需求和新应用场景不断增加新产品和解决方案。目前公司在全国各省市自治区设立六十多家分支机构，拥有覆盖全国的分销渠道和售后服务体系。

图表2： 公司主要产品分类

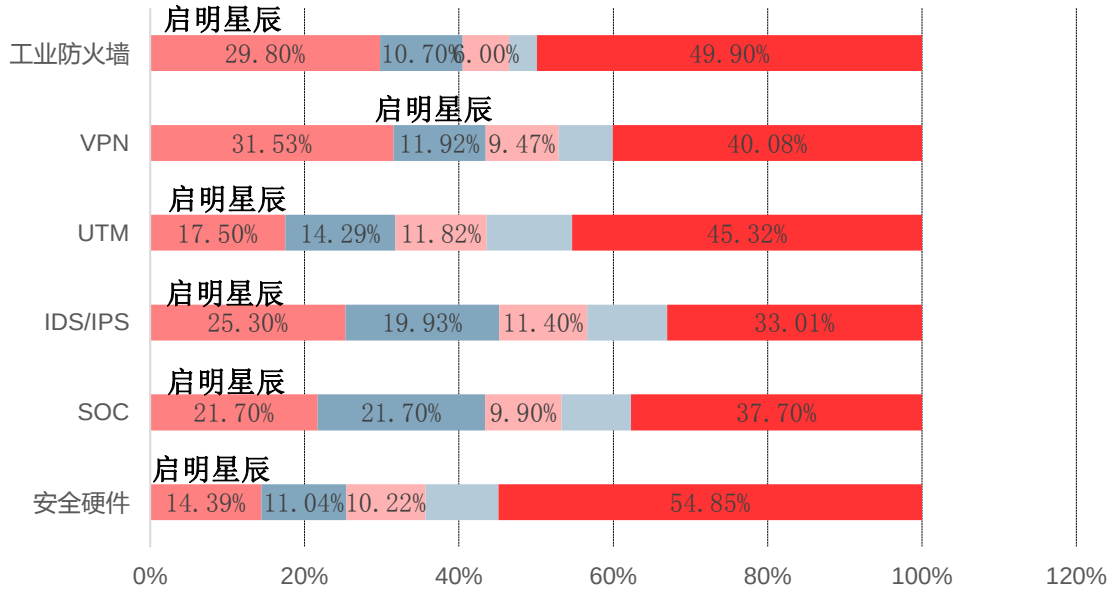
产品大类	介绍	典型产品与服务
安全网关	部署于网络边界、出口，兼具用户认证、访问控制、NAT、SAML 众多功能的综合性 VPN 安全网关，可为各种规模的企业、政府机构、军队、团体提供网络数据加解密服务，最大限度的保护用户网络传输的数据安全	防火墙、 NGFW、 UTM、 VPN 网关、网闸、抗 DDoS 等
安全检测	部署于网络内部中深层。又可细分为入侵检测（IDS）和入侵防御（IPS），其中 IDS	IDS/IPS、网络审计、内网安全管理

产品大类	介绍	典型产品与服务
	的作用是帮助用户量化、定位来自内外网络的威胁情况，提供有针对性的指导措施等和安全决策依据，并能够对网络安全整体水平进行效果评估；IPS 通过对网络中深层攻击行为进行准确的分析判断，在判定为攻击行为后立即予以阻断，主动而有效的保护网络的安全	
数据安全与平台	以数据为基础或对象。系统以“旁观者”的方式观察和记录员工对电脑、文件、软件操作或网络行为，同时服务端通过多种方式（文件签名、敏感词识别与权重分析、正则表达式过滤）识别敏感机密信息。并通过数据汇总与分析，得出人员、文件、安全事件这三个维度的趋势，并通过相应的安全策略定义，对用户的操作进行识别，从而确认泄密风险并采取相应措施进行防范	SOC、 4A、 DLP、数据管控、大数据处理分析等
安全服务与工具	输出安全能力，为客户提供的相关服务与工具。启明星辰通过对用户常见的信息安全面临的外部及内部需求进行总结，结合自身多年的服务经验，以客户需求为导向建立起一套整体安全服务产品体系。	风险评估、监控应急、安全运维、产品售后、安全培训等服务以及相关工具类产品
硬件及其他	为用户提供安全解决方案、系统集成项目所用。产品即 基于多核硬件平台的高性能 UTM 产品，并且该部分产品市场较为成熟、竞争激烈	第三方软、硬件等

资料来源：公司官网，中信建投证券研究发展部

公司在多个网络安全子领域保持市占率第一或领先。自 2002 年起，启明星辰持续保持国内入侵检测、漏洞扫描市场占有率第一；近年来公司已经发展成为国内统一威胁管理 UTM、工业互联网信息安全管理系统(工业 SOC)、工业防火墙国内市场第一位，并成为安全性审计、安全专业服务、工业互联网/物联网安全、私有云/专有云/行业云等新市场领导者，公司也是唯一一家在所有安全网关类细分市场都名列前茅的企业。公司明星产品包括：天清汉马 T 系列防火墙、天清汉马 USG 一体化安全网关、天阗入侵检测与管理系统、天清入侵防御系统、天清汉马工业防火墙 IFW-3000 系列、网御防火墙、工业互联网信息安全管理系统等。

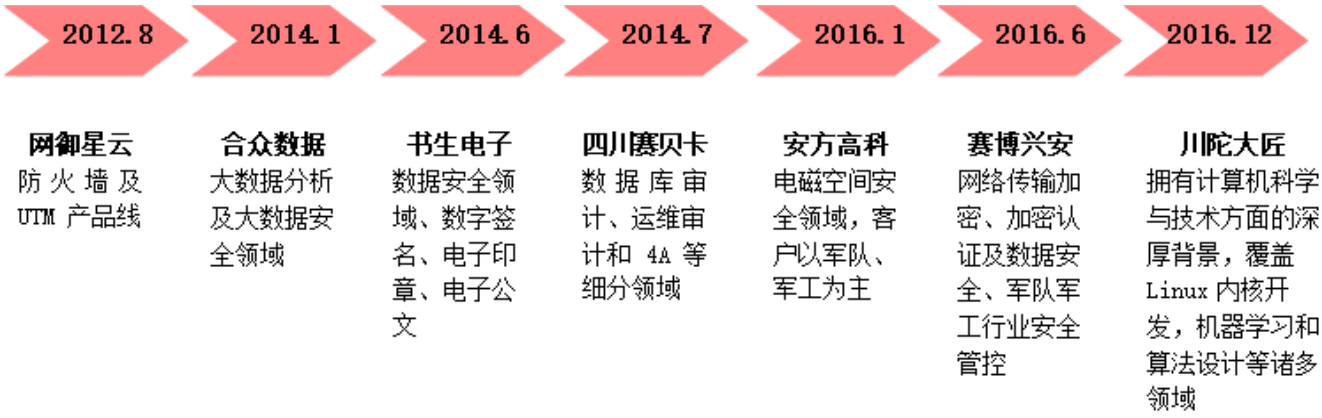
图表3： 2018 年启明星辰产品在各细分领域市占率



资料来源：IDC，中信建投研究发展部

锐意进取，外延并购助力网络安全多领域覆盖，初步形成网络安全产业生态圈。在自身传统业务保持领先的同时，公司不断打破自身局限，通过外延并购拓展新市场和领域并取得了优异业绩。2014 年，公司收购书生电子 100%股权，合众信息 51%股权，四川赛贝卡 100%股权，对数字签名、电子印章、数据库审计及大数据分析和大数据安全领域进行布局；2015 年，收购安方高科 100%股权，拓宽了在电磁兼容和信息安全防护工程方面的业务；2016 年，收购赛博兴安 90%股权、川陀大匠 85%股权，加强了公司在网络安全管理与监察、安全检测和移动信息安全等领域的业务能力，进一步拓展军工市场。从已披露的并购子公司的业绩来看，网御星云为公司收入和利润贡献最大，2018 年其营收为 7.84 亿元，占公司总营收 31.1%，净利润为 1.27 亿元，占公司净利润 22.32%；赛博兴安 2018 年营收为 1.68 亿元，占公司总营收 6.66%，净利润为 0.59 亿元，占公司净利润 10.37%。此外公司还逐步投资了一大批在新兴网络安全产品和 IoT、IT 领域布局的优秀公司，逐步实现了对网络安全、数据安全、应用业务安全、IoT 安全等多领域的覆盖，初步形成了信息安全产业生态圈。

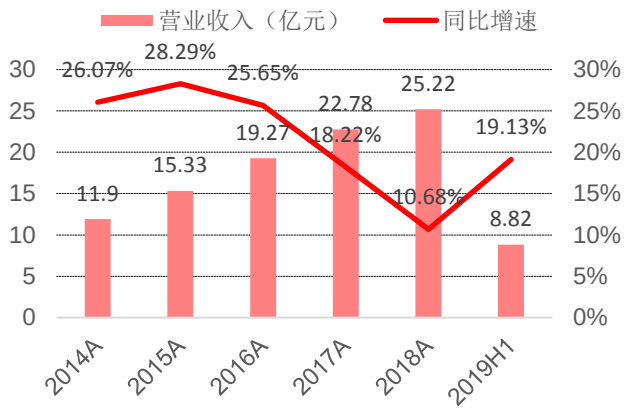
图表4： 公司通过外延并购助力快速发展



资料来源：公司公告，中信建投研究发展部

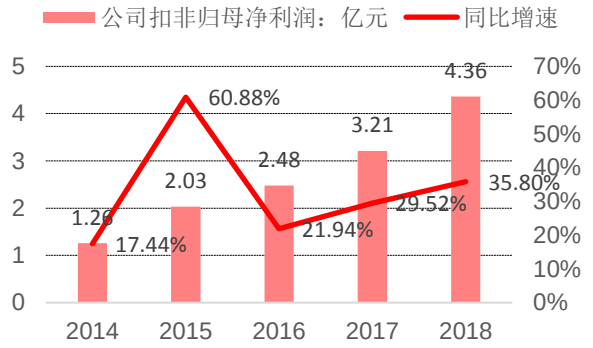
多年营业收入和净利润保持连续增长，财务表现稳健。2018 年公司实现营收 25.21 亿元，同比增长 10.68%；归属母公司所有者净利润为 5.68 亿元，同比增长 25.9%。2019 年上半年，公司实现营收 8.82 亿元，同比增长 19.13%，主要是因为党政军客户业务五年周期过半带来的需求加速释放（2019~2020 年是十三五规划最后两年），使得收入较去年同期有大幅度回升。自 2014 年至 2018 年，公司营收复合增长率 20.5%，扣非归母净利润从 1.26 亿元增长至 4.36 亿元，复合增长率 36%，其中 2019 年 H1 归母净利润同比下降 40.97%，主要原因为去年同期确认参股公司恒安嘉新的投资收益金额较大，归属于母公司所有者的扣除非经常性损益的净利润为-210 万元，同比增长 96.92%。

图表5： 启明星辰近五年营业收入及同比增速



资料来源：Wind，中信建投研究发展部

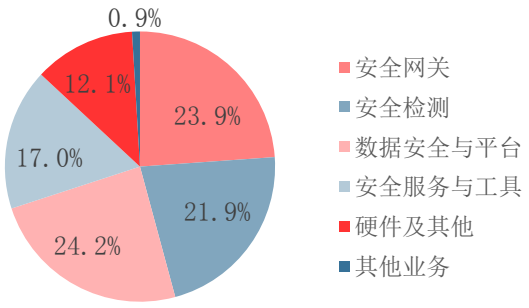
图表6： 启明星辰近五年扣非归母净利润及同比增速



资料来源：Wind，中信建投研究发展部

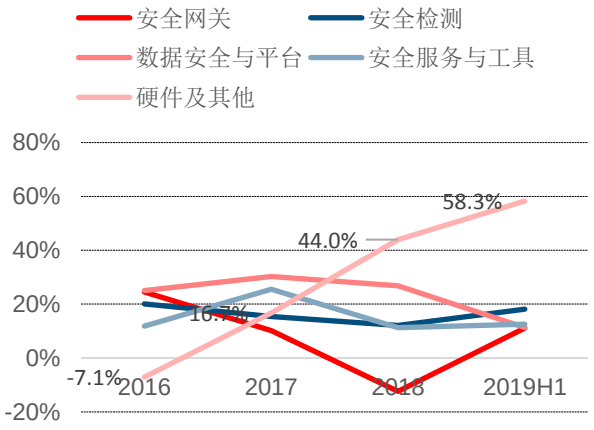
公司收入结构多元，数据安全和硬件收入近年快速增长。综合近几年来看，公司安全网关类产品对收入贡献最大，2018 年占总营收 23.88%，较同期有所减少，2019H1 占总收入占比为 34.03%。安全检测业务 2018 年占总收入比例为 21.91%，近三年增长较平稳，维持在 15%—20%同比增速。数据安全与平台近年增速较快，由于大数据和移动互联网的高速增长，与之相关安全服务业务、数据平台也保持高速增长， 2018 年公司在智慧城市安全运营、 工业互联网安全等战略新业务方面发展成效显著，也有力带动了数据安全与平台业务的快速增长。近年安全服务逐渐被越来越多的用户认可和接受，公司安全服务与工具板块收入保持增长，2018 年占总收入 16.95%，同比增长 11.28%。公司硬件及其他业务的收入较去年同期相比涨幅最大，主要原因是来源于公司 2018 年以后进入了新的行业和客户领域，系统集成项目的增长，因此硬件及其他业务收入增长明显加速。

图表7： 启明星辰 2018 年主营业务收入构成



资料来源：Wind，中信建投研究发展部

图表8： 启明星辰各类产品营收增速

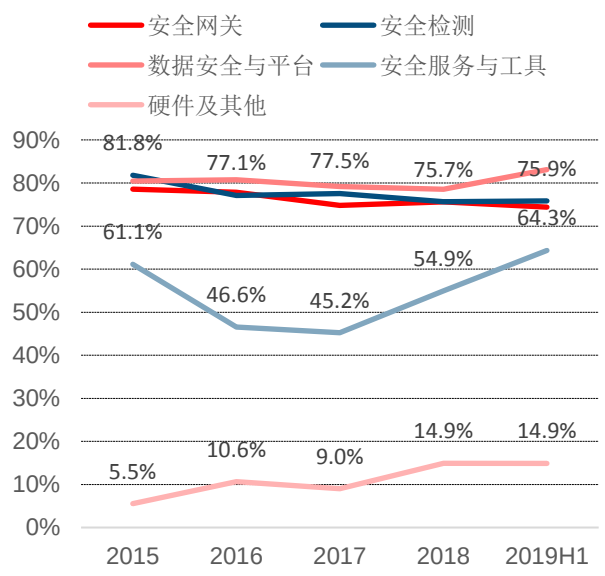


资料来源：Wind，中信建投研究发展部

产品附加值高，传统产品品牌优势大，公司综合毛利率维持高水平。由于公司产品科技含量高，产品具有行业领先性且具有较高的产品附加值，因而综合毛利率一直维持高位，2015 年至 2019 年上半年，公司的综合毛利率分别为 69%、67%、66%、66%、64%。其中公司核心产品安全网关和安全检测毛利率较高且贡献最大，毛利率保持在 75%以上，两者毛利贡献加起来超过 60%，近年毛利率略降主要原因是随着原材料成本的逐渐攀

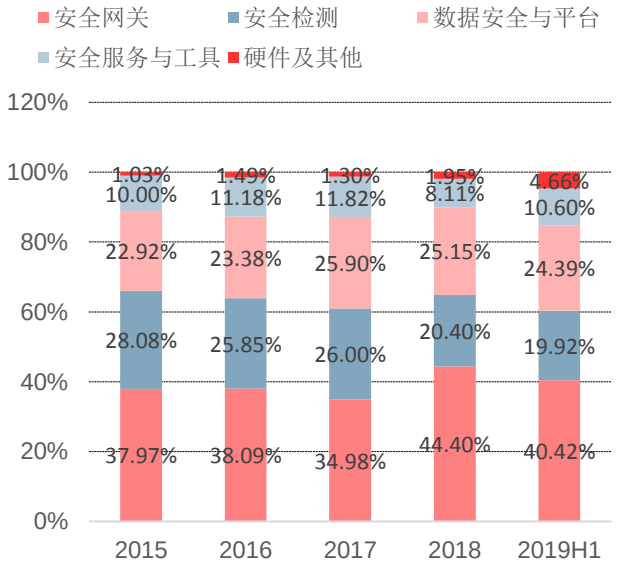
升，而安全网关和安全检测业务的销售价格保持基本稳定，所以毛利被挤压。数据安全与平台的毛利率接近 80%，是公司所有产品最高的，且毛利增长较快，2018 年毛利贡献已经超过了安全检测业务，盈利能力较强，主要原因是公司拥有完善的专业安全产品线和强大的信息安全专家团队，由此能够形成公司的整体优势与竞争壁垒，也为公司在大数据安全和移动互联网的发展奠定良好基础。安全服务与工具业务的毛利率一直处于 50%较高水平。公司安全服务与工具业务主要有风险评估、监控应急、安全运维、产品售后、安全培训等服务以及相关工具类产品。2016 年公司安全服务毛利率下降到 46.58%，主要原因是收购安方高科所致， 安方高科属于电磁信息安全防护行业，包括抗电磁干扰、介质保护和电磁泄漏防护等，毛利率大约为 25%~30%，公司将其划分为安全服务与工具业务，使安全服务与工具业务的毛利率整体下降。公司硬件及其他产品类别占公司毛利金额和比例均较小，硬件及其他为第三方外购产品，主要是网络安全解决方案中集成了其他厂商的产品，并且该部分产品市场较为成熟、竞争激烈，因而毛利率也较低，占公司整体毛利比重不超过 5%，对公司整体毛利影响较小。

图表9： 启明星辰各项业务毛利率情况



资料来源：Wind，中信建投研究发展部

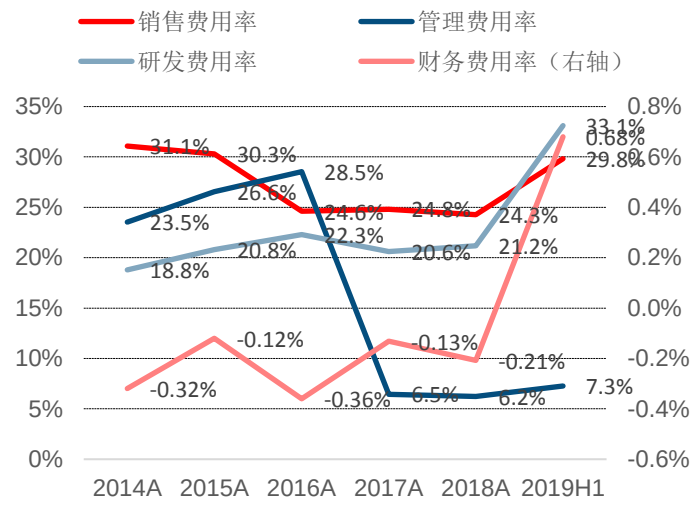
图表10： 启明星辰各业务毛利率贡献占比



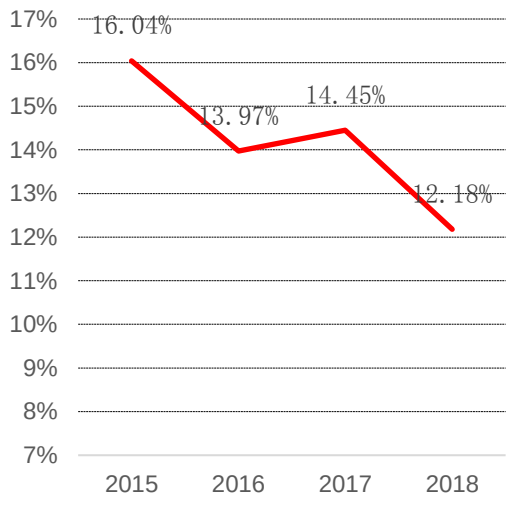
资料来源：Wind，中信建投研究发展部

公司费用率总体稳定，研发投入持续加大。销售费用率自 2016 年开始下降，主要源于并购后销售渠道的整合使得销售费用率下降。公司结合市场的需求和战略发展要求，在继续加强完善原有系列产品功能与性能升级改造基础上，加大研发创新投入，2015 年以后公司研发费用率均在 20%以上且逐年上升，2019H1 研发费用率为 33.11%，研发投入同比增加 4.48%，主要投入于“安全中台”建立、城市安全运营业务基础建设、云安全资源池及关联安全管理平台和运营服务业务等。过去几年公司员工人数和研发人员也持续增长，2018 年员工总人数为 3863 人，其中技术人员（包含部分研发人员）占员工总人数比例为 59.57%， 2018 年研发人员同比增长 16.5%，占总员工总数比例达到 42.58%。2018 年职工薪酬总额为 1.38 亿元，占公司成本总额的 15.80%。公司核心技术人员数量为 90 人，占全体员工总数的 2.33%，薪酬占全体员工薪酬总额的 6.63%。

图表11： 启明星辰近年费用率变化情况



图表12： 启明星辰资本化研发投入占研发投入的比例

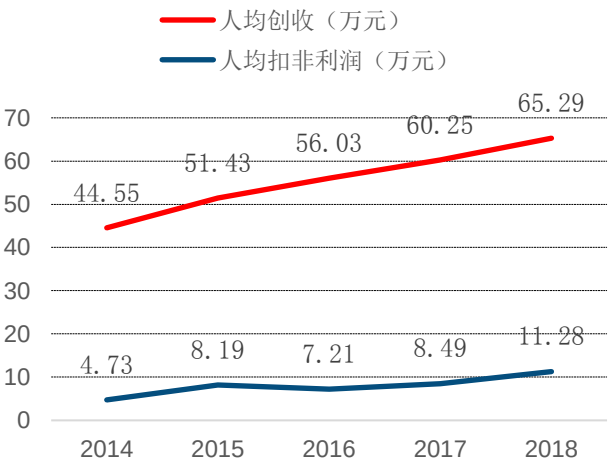


资料来源：Wind，中信建投研究发展部

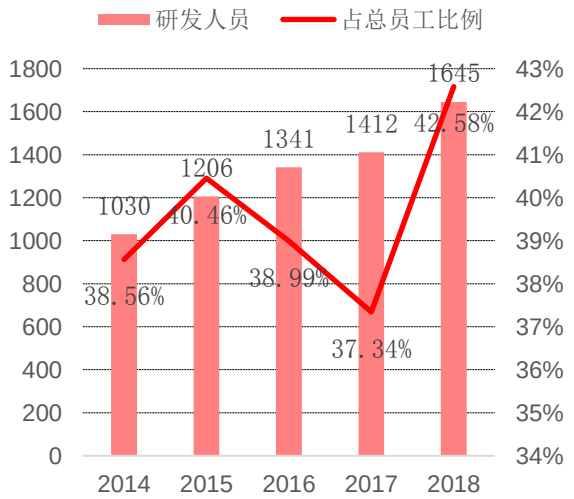
资料来源：Wind，中信建投研究发展部

公司拥有代表国内最高水准的技术团队和超过 400 项技术专利。目前公司拥有包括积极防御实验室（ADLab）、核研院、产品研发中心、泰合团队、北斗安全运营中心、VenusEye 威胁情报中心、VF 安全咨询专家团、云安全团队、工业安全团队、安全系统集成团队等，构成了公司重要的核心竞争力。公司拥有我国规模最大的国家级网络安全研究基地，拥有国家专利 400 余项（其中 60 余项填补了国内信息安全领域的空白）和计算机软件产品著作权近 300 项，牵头/联合参与制订国家及行业网络安全标准近 30 项，完成包括国家发改委产业化示范工程、科技部 863 计划、国家科技支撑计划、核高基重大专项、工信部产业发展基金项目等国家级科技攻关项目 200 余项。

图表13： 启明星辰人均创收和人均扣非净利润变化情况



图表14： 启明星辰研发人员情况



资料来源：Wind，中信建投研究发展部

资料来源：Wind，中信建投研究发展部

公司人均创收能力持续增长，人均扣非净利润稳步增长。从 2014 年至今公司人均创收一直保持逐年增长的趋势，2016 年人均创利有所下降的原因主要是主要原因是收购安方高科所致。从人均创收和人均创利总体趋势

来看，公司新产品和解决方案的推出、新市场领域的覆盖以及投资并购生态圈的建设被证明较为成功。

公司员工持股计划已执行两期，充分调动员工积极性，目前公司正回购股份继续用作股权激励或员工持股计划。公司至今已做了两期员工持股，其中，第一期非公开发行 690.45 万股，认购价格 10.79 元/股，于 2019 年 1 月 25 日上市流通，2020 年 1 月 14 日届满。截至 7 月 12 日最新公告披露，公司第一期员工持股计划持有公司 470.54 万股，占公司总股本的 0.52%。第二期员工持股计划非公开发行，495.03 万股，认购价格 20.03 元/股，2017 年 1 月 19 日上市，锁定期三年至 2020 年 1 月 19 日，存续期为 4 年。目前，公司正通过回购股份用作股权激励或员工持股计划，截至 10 月 10 日，已回购 412.52 万股，占公司总股本的 0.46%，总成交金额为 9998 万元，已基本接近公司目标回购总金额（0.5 至 1.5 亿元）和回购股份数（250 万股至 500 万股）。通过员工持股计划，公司将充分调动员工积极性，推动公司持续发展。

图表15： 公司员工持股计划情况

	非公开发行股票数(万股)	认购价格(元/股)	上市日期	解除限售并上市流通	存续期结束日期
第一期员工持股计划	690.45	10.79	2016.01.25	2019.01.25	2020.01.14
第二期员工持股计划	495.03	20.03	2017.01.19	2020.01.19	2021.01

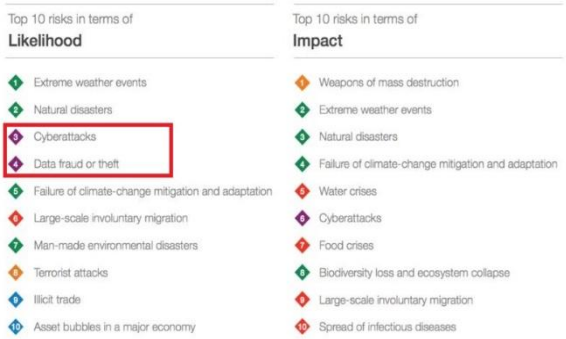
资料来源：公司公告，中信建投证券研究发展部

二、网络安全占信息化支出占比将逐步提升，行业需求变化和技术变革促进网络安全行业增速加速

2.1 网络安全威胁事件频发，国家安全受到挑战，中国网络安全占信息化支出占比将逐步提升

网络安全威胁事件频发，没有网络安全就没有国家安全。2018 年 1 月世界经济论坛最新发布的《全球风险报告》，阐述了全球企业所面临的风险，网络攻击和数据泄露排在最有可能发生的前五大风险第三位、第四位，首次进入前五大威胁。网络攻击、病毒爆发和数据泄露事件近年在全球范围内出现越来越频繁，涉及各行各业，大到全球化公司、大型互联网企业，小到城市医保系统，如已公开的 12306 网站、医疗行业患者信息、A 站、顺丰快递、华住酒店、万豪酒店、陌陌等；高危漏洞层出不穷，如英特尔处理器“Meltdown”和“Spectre”新型漏洞、ThinkPHP 漏洞、移动支付 SDK 漏洞、思科漏洞等；Web 攻击依然常见，除利用 Struts2 系列漏洞、Weblogic 漏洞进行的攻击外，还有因 WebAPI 的广泛普及与使用导致的攻击事件；APT 攻击如海莲花依然活跃； 挖矿与勒索病毒攻击持续不断，如 MsraMiner 挖矿病毒、XMRig 挖矿木马、Globelmposter/GandCrab 勒索病毒、Lucky 跨平台 勒索病毒、Oracle 数据库比特币勒索病毒、Wannacry 勒索病毒等。网络安全是经济全球化和社会信息化的前提，也是国家安全和社会稳定的基础，没有网络安全就没有国家安全，因此各国政府、企业都提高了对网络安全的重视。

图表16： 2018 年世界经济论坛将网络攻击、数据泄露首次列入全球企业所面临前五大风险



资料来源：财富杂志，中信建投证券研究发展部

图表17： 2017 年全球各区域网络犯罪造成损失（亿美元）

地区（世界银行统计）	区域 GDP（千亿美元）	网络安全损失（十亿美元）	网络安全损失 GDP 占比
北美	20.2	175	0.87%
欧洲和中亚	20.3	180	0.89%
东亚	22.5	200	0.89%
南亚	2.9	15	0.52%
拉丁美洲	5.3	30	0.57%
撒哈拉以南非洲	1.5	3	0.20%
中东及北非	3.1	5	0.16%
全球	75.8	608	0.80%

资料来源：国家互联网应急中心，中信建投证券研究发展部

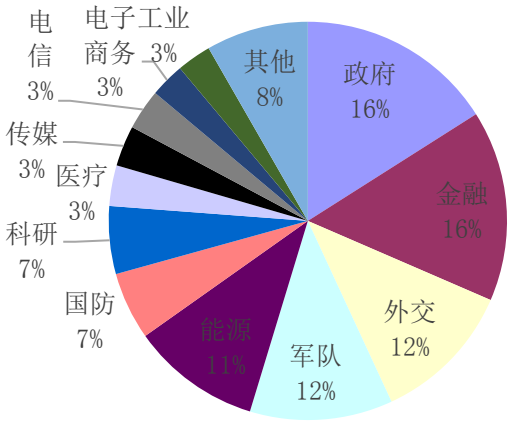
网络安全威胁造成的经济损失越来越多，国家对网络安全重视程度进一步提高。Frost＆Sullivan 和微软的研究表明，网络安全问题给全球造成的损失 2017 年高达 6000 亿美元，预计 2021 年将增至 1 万亿美元，遭受网络攻击数据泄露或者病毒勒索，造成的直接经济损失包括企业的收入、生产力、罚款、诉讼和补救措施；间接损失包括客户流失、声誉受损等。根据国家互联网应急中心调查中可以看出网络安全带来的损失在北美、欧洲还有东亚等信息化程度较高的区域最高，每年网络安全造成的经济损失超过 5500 亿美金，平均占到 GDP 的 0.85%以上。

网络空间战日益成为大国战略博弈的新战场，国家安全作为网络安全中最重要的组成部分，加强网络安全能力建设和投入才能匹配我国的大国地位。无论是发动 APT 攻击，还是披露 APT 攻击，均成为了现代国际关系中，大国政治与战略博弈的重要棋子，而整个网络空间就是大国战略博弈的新战场。美俄两国，特别是美国，非常善于通过公开威胁事件及情报共享等方式，对其他国家施加政治压力，打击其他国家经济或者政治稳定性。过去美国的“震网”（Stuxnet）系统连续多年对伊朗进行 APT 网络攻击，该系统由美国国家安全局在以色列协助下研制。据估计美国对伊朗核工厂的网络袭击共破坏 984 个浓缩铀离心机，导致伊朗提炼浓缩铀能力下降 30%。而根据我们产业调研发现，中美贸易摩擦持续升级背后，中美间的网络攻击局势也日益紧张，APT 攻击次数和频率明显提升。目前我国在网络安全领域投入还较少，网络安全市场整体规模和美国相比仍然有较大差距，未来国家必须要加强网络安全能力建设和投入才能匹配现在的大国地位。

图表18： 2019年上半年遭受APT攻击后感染专用木马用户最多的省级行政区依次是：广西、北京、辽宁、云南、海南、四川，也和我国企业信息化程度相关

资料来源：360 网络安全研究院，中信建投证券研究发展部

图表19： 2018年中国境内遭受APT攻击的行业分布



资料来源：360 网络安全研究院，中信建投证券研究发展部

“云大物移”新场景驱动下防护对象改变，企业网络边界逐渐消失，政府和企业网络安全防护理念发生较大变化，网络安全不再是“补丁”模式，而是与信息系统建设同时规划，促进信息安全占 IT 支出占比逐步提升至 5%以上。2015 年以前政企部署网络安全产品都在基础信息化部署完成之后，像打“补丁”一样将边界安全产品加到整体信息系统中进行防护和防御，因此网络安全投资占信息化整体投资比例一直低于 2%。**2015 年以后，随着新的应用场景云计算、大数据、物联网和移动终端的普及，企业信息化程度逐步提升，网络安全领域出现了三大变化：**

1）防护对象改变：从传统 PC、服务器、网络边缘到云计算、大数据、泛终端、新边界；

2）防护思想变化：从“风险发现、查缺补漏”到“关口前移、系统规划”；

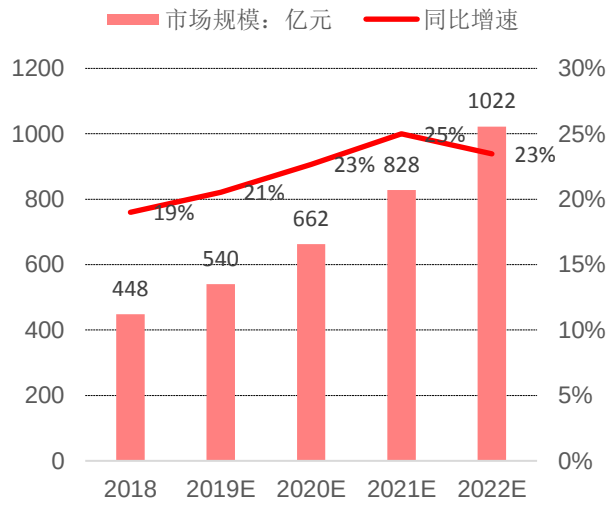
3）核心技术升级：从传统的围墙式防护到利用大数据等技术对安全威胁进行检测与响应

正是企业信息如今企业的信息网络边界逐步消失，网络安全必须和信息系统建设同时规划。数字经济给了企业安全一次新的机会，在数字化过程中把安全内置进信息系统，因此未来网络安全投资有望占 IT 信息支出占比达到 5%以上。2019 年预计中国网络安全市场规模将达到 540 亿，保持 21%的增长速度，IDC 预计 2019~2021 年中国网络安全市场年复合增速将超过 23%。

图表20： 国家安全与政企数字化转型给网络安全领域提出了新的要求，网络安全领域出现的三大变化

资料来源：360 企业安全，中信建投证券研究发展部

图表21： 中国网络安全市场规模在 2019 年达到 602 亿规模，保持 21%的增长速度（单位：亿元）



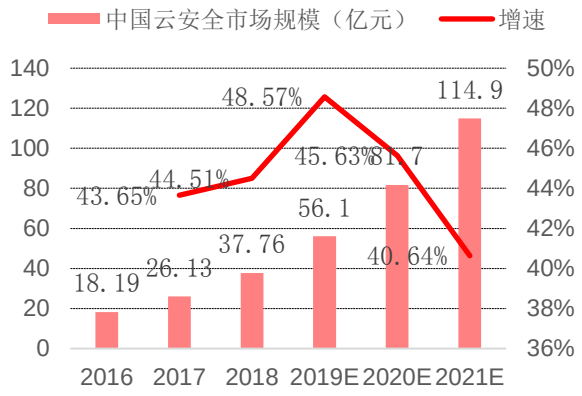
资料来源：IDC,中信建投证券研究发展部

2.2“云大物移”等新场景和新技术促进信息安全行业发展加速，网络安全新产品和新解决方案层出不穷

随云计算快速增长，云安全需求持续爆发。根据中商产业研究院数据显示，2018 年中国云安全市场规模达 37.76 亿元，增长 45%。随着信息安全越来越受到重视，云安全市场将进一步扩大。预计 2019 年，中国云安全市场规模将达 56.1 亿元，增长近五成。到 2021 年，预计我国云安全市场规模将超 100 亿元。以启明星辰中报的政务云平台为例，安全解决方案占整个政务云订单的 20%，而其中云安全占 10%左右。

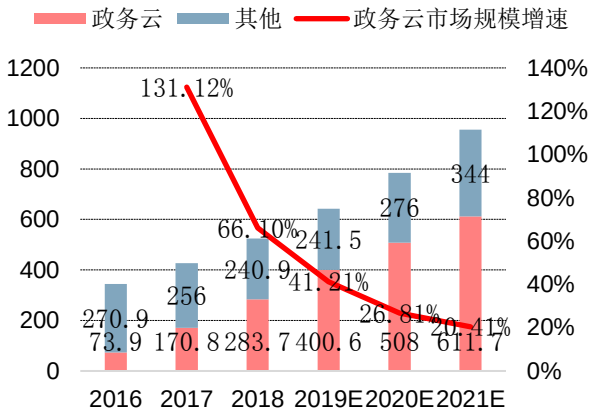
目前的云安全领域有几大方向：1)云计算和网络安全：主要研究如何保障云自身及云上各种应用的安全，包括云计算机系统安全、用户数据的安全存储与隔离、用户接入认证、信息传输安全、网络攻击防护、合规审计等；**2)安全基础设施的云化：**主要研究如何采用云计算新建与整合安全基础设施资源，优化安全防护机制，包括通过云计算技术构建超大规模安全事件、信息采集与处理平台，实现对海量信息的采集与关联分析，提升全网安全事件把控能力及风险控制能力；**3）数据安全**：在云计算环境中的业务数据自身的安全管理，包括收集与识别、分类与分级、权限与加密等方面；**4)云安全服务：**主要研究各种基于云计算平台为用户提供的安全服务，如防病毒服务等。

图表22： 中国云安全市场规模及增速



资料来源：IDC，中信建投证券研究发展部

图表23： 中国私有云市场规模（亿元）



资料来源：中国信通院，中信建投证券研究发展部

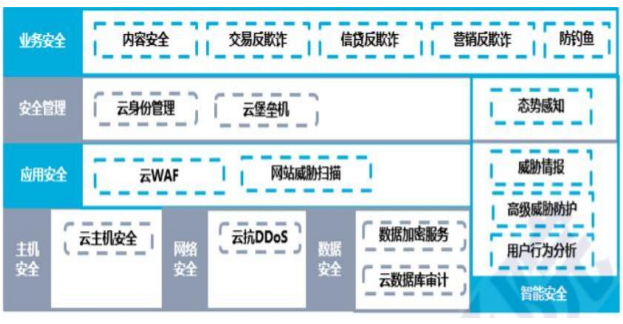
公有云安全中，云计算提供商需要进行完整的安全体系建设，一般包括以下八个层次：业务连续性管理防护、物理安全防护、云安全防护、网络安全防护、主机安全防护、数据安全防护、应用安全防护、业务安全防护。而用户使用的云服务层面不同，安全责任不相同。如果用户只是使用 IaaS 层的服务，IaaS 层安全由云服务商提供，之上的所有中间件以及业务安全责任全部由用户自己承担；如果使用的是 SaaS 层的服务，云服务商就要提供云相关全栈的服务；PaaS 层的情况介于这两者之间。1）IaaS 云服务提供商主要负责为用户提供基础设施服务，如提供包括服务器、存储、网络和管理工具在内的虚拟数据中心，云计算基础设施的可靠性、物理安全、网络安全、信息存储安全、系统安全是其基本职责范畴，包括虚拟机的入侵检测、完整性保护等； 2）PaaS 的安全主要分以下几个维度为进行保障：功能安全、运维安全、OpenAPI 安全、基础设置安全（IaaS）和容器、镜像安全。其中功能安全包括多租户隔离、多租户资源管理、身份认证和访问控制、单点登录、PSM 秘钥管理系统以及数据安全等具体功能。PaaS 云服务提供商主要负责为用户提供简化的分布式软件开发、测试和部署环境，云服务提供商除了负责底层基础设施安全外，还需解决应用接口安全、数据与计算可用性等； 3）SaaS 云服务提供商需保障其所提供的 SaaS 服务从基础设施到应用层的整体安全。应用安全目前较为成熟的产品包括云 WAF 保护、网站威胁扫描。数据安全主流产品则包括数据加密服务、云数据库审计等。同时云计算厂商还提供内容安全、交易反欺诈、信贷反欺诈、营销反欺诈和防钓鱼等安全产品。

图表24： 云安全层次和产品分类

IaaS	PaaS	SaaS
数据安全	数据安全	数据安全
终端安全	终端安全	终端安全
访问控制管理	访问控制管理	访问控制管理
应用安全	应用安全	应用安全
主机和网络安全	主机和网络安全	主机和网络安全
物理和基础架构安全	物理和基础架构安全	物理和基础架构安全

资料来源：腾讯云，中信建投证券研究发展部

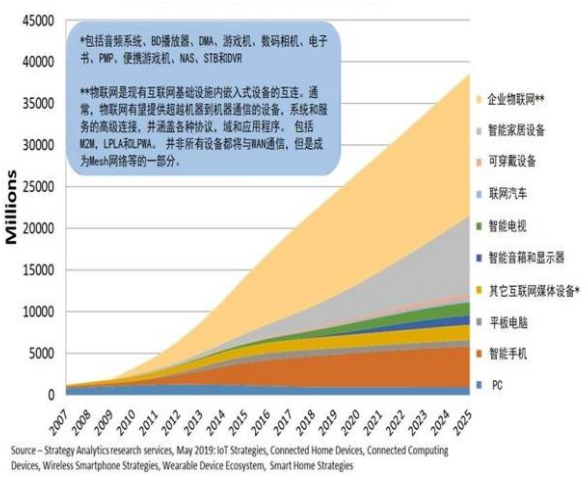
图表25： 云安全产品体系



资料来源：中国信通院，中信建投证券研究发展部

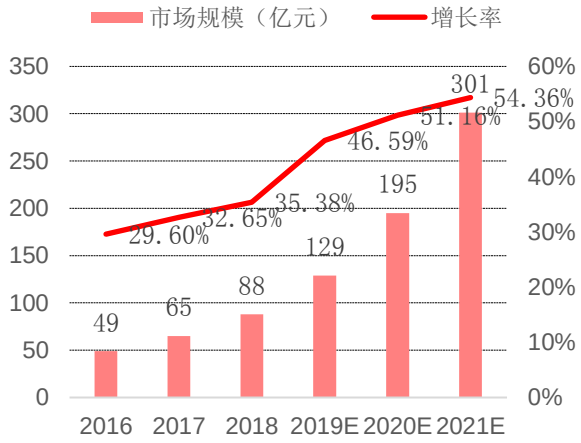
中国市场私有云规模较大且增速较快，未来国内私有云/混合云安全市场空间广阔。云安全能力对厂商统一管理、全局视角和从上至下整体规划部署能力提出更高要求。由于国情和文化差异，中国私有云处于主导地位，且政务云目前占比较高，根据信通院数据，2018 年中国云计算市场共 963 亿元，其中私有云 525 亿元，占比 55%，而国内的政企云也大多是私有云/混合云架构为主。根据信通院 2018 年的调查报告显示，有 44%的私有云安全投入比例不到 5%，比例较低，私有云和混合云的网络安全重视程度和市场规模还有较大提升空间。私有云的安全产品和服务方面，通过第三方安全公司提供安全服务的比例为 54.4%，另外有 41%的私有云服务商自己提供。与传统网络安全不同之处在于，云计算的基本架构虚拟化系统自身存在一定的安全危险，攻击者通过一些漏洞可以窃取虚拟机的资源，同时云计算架构数据比较集中，事故一旦发生影响范围比较大，后果较为严重，且在云环境中数据安全和应用安全防护技术难度和要求更高。

图表26： 全球物联网设备接入量（百万）



资料来源：Strategy Analysis,中信建投证券研究发展部

图表27： 中国物联网安全市场规模和增速

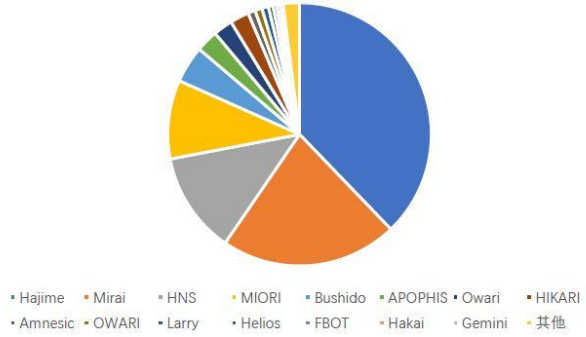


资料来源：中商产业研究院，中信建投证券研究发展部

物联网安全问题日益严峻。随着 5G 网络技术发展，预计 2021 年将会有 251 亿物联网设备接入互联网，年增长率 32%。随着物联网连接数快速增长，物联网安全事故也成为关注重点。一是由于物联网设备的实时在线性使得它们天生具备成为“肉鸡”的潜力；二是由于物联网设备制造商在安全开发商投入较少导致物联网设备容易受到攻击；三是针对物联网设备的攻击很难被发现，反而人的 PC、服务器由于经常需要进行人机交互，一旦出现异常情况可以迅速被发现并进行处理；四是物联网设备更新较慢，大量物联网设备无法及时获得固件更新，导致新补丁也无法校友使 IoT 设备得到保护。过去一年针对 IoT 设备的攻击增长迅猛，众多物联网设备成为巨大僵尸网络中的节点，并被用来发动 DDoS 攻击、当做跳板攻击其他机器、挖矿、劫持网络流量等。同时我们发现 2018 年重要行业关键信息基础设施逐渐成为勒索软件的重点攻击目标，涉及政府、医疗、教育、研究机构、制造业等。据 VenusEye 威胁情报中心数据，2018 年捕获的各类受僵尸网络控制 IoT 设备，中国占比达到 21.49%最多，其次是俄罗斯（16.03%）、巴西（5.65%）。且 IoT 蠕虫家族从 2017 年 10 种快速增加到 2019 年的 19 种，物联网安全问题日益严峻。

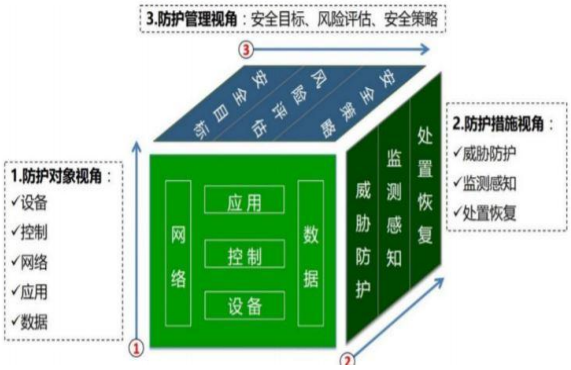
随着物联网市场的体量的不断扩大，物联网安全市场也将迎来快速发展。据中商产业研究院数据显示，2018 年中国物联网安全市场规模超 88 亿元，同比增长 35%。随着市场持续增长，预计 2019 年物联网安全市场规模将近 130 亿元，到 2021 年，物联网安全市场规模将超 300 亿元，行业保持较高的年复合增速。按照应用场景分析，物联网安全覆盖：消费级物联网（如智能家居、智能穿戴设备安全）、车联网安全（以车内网、车际网和车载移动互联网安全）、工业互联网安全和产业互联网安全。

图表28： IoT 流行蠕虫家族



资料来源：启明星辰网络安全态势报告，中信建投证券研究发展部

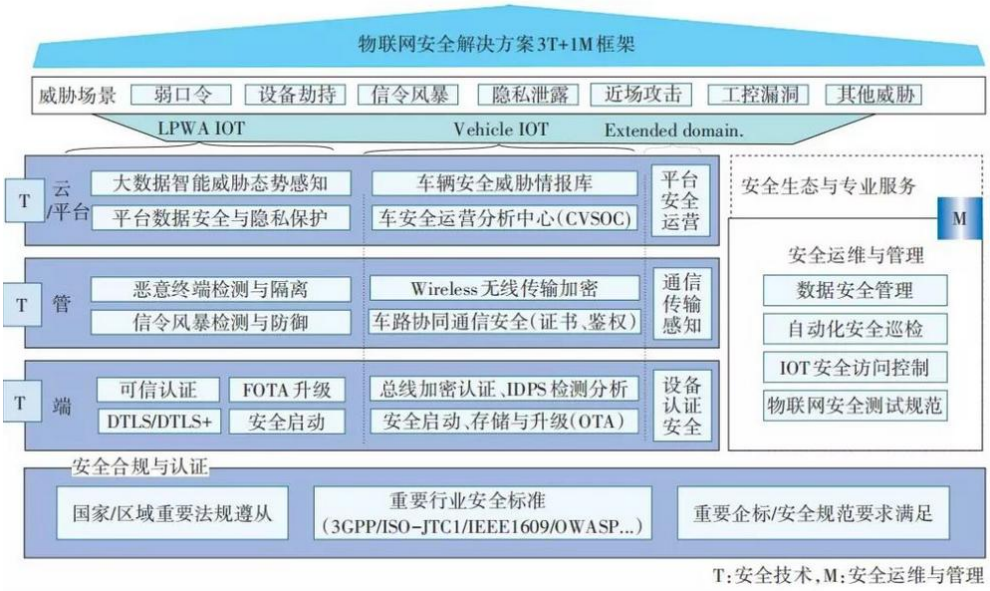
图表29： 工业互联网安全防护框架



资料来源：中国工业互联网安全态势报告，中信建投证券研究发展部

物联网安全包括应对感知层、网络层和应用层的安全威胁，核心在于基于物联网应用场景安全威胁，构建起终端防御、管道保障、云端保护 3 个层级的物联网安全以及安全运维与管理。构建终端安全体系是保证物联网安全的第 1 道防线。由于物联网应用行业多，需要针对不同场景、不同类型的终端进行设计，根据终端环境和处理能力进行区分，匹配与其计算资源和应用相适应的安全技术。网络是物联网安全的第 2 道防线。物联网终端由于自身防护能力较弱，可以考虑如何在网络和平台侧海量的终端和数据中，对恶意行为进行快速检测，并迅速做出判断和相应，进行报警和隔离处置。利用运营商的网络能力，在网络侧提供安全监控服务，是运营复杂度最低、建设成本最低、对业务影响最小同时也是最实际有效的防护方案。平台和数据是物联网安全的第 3 道防线，云端平台及数据的防护包括平台安全、数据存储、处理、传输、开放环节中的安全与隐私保护等。

图表30： 物联网安全解决方案



资料来源：华为物联网安全白皮书，中信建投证券研究发展部

2.3 等保 2.0 针对新场景新技术提出新要求，加速网络安全产品、解决方案发展

2017 年 6 月《网络安全法》正式实施后，对违法网络安全法规的政府机关、企业处罚力度增加，促进企业合规性采购需求增加，2019 年 5 月等保 2.0 正式发布，进一步促进 2019 年~2021 年信息安全市场快速增长。

等保 2.0 新变革针对共性安全保护需求提出安全通用要求；针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护标准。1）新增防护对象，除了传统基础信息网络防护，新增对云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等。同时国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。2）增加扩展要求：新增加云计算安全扩展要求，主要增加了虚拟网络之间安全隔离、虚拟化安全监测、虚拟机之间资源安全隔离、云计算环境安全管理、数据安全、剩余信息保护、镜像快照保护，对物理资源和虚拟资源按照策略做统一管理调度与分配等安全管控。新增移动互联安全扩展要求，主要包括无线边界控制、入侵防范、移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发、配置管理等安全要求。3）新增感知节点设备安全、区域边界接入控制、入侵防范、抗数据重放、数据融合处理、感知节点运维管理等安全要求。调整安全管理策略，形成管理体系；4）增加安全管理中心，提高监测预警水平。在“第二级”开始增加“安全管理中心”的“系统管理”和“审计管理”要求。在“第三级”调整了系统管理、审计管理、安全管理及集中管控。

图表31： 等保 1.0 和等保 2.0 对比

		等保 1.0	等保 2.0
通用要求	等级保护对象	信息系统	物理安全、网络安全、主机安全、应用安全、数据安全和备份与恢复
	管理要求	安全管理制度	安全策略与管理制度
		安全管理机构	安全管理机构和人员
		人员安全管理	
		系统建设管理	安全建设管理
		系统运维管理	安全运维管理
	技术要求	物理安全	物理和环境安全
		网络安全	网络和通信安全
		主机安全	设备和计算安全
		应用安全	
		数据安全与备份恢复	应用和数据安全
		存在安全控制点的 S/A/G 标注	不存在安全控制点的 S/A/G 标注
新技术安全扩展要求	云计算安全扩展要求		基础设施的位置、虚拟化安全保护、镜像和快照保护、云服务商选择和云计算环境管理
	移动互联安全扩展要求		无线接入点的地理位置、移动终端管控、移动应用管控、移动应用软件采购和移动应用软件开发
	物联网安全扩展要求包括		感知节点的物理保护、感知节点设备安全、感知网关节点设备安全、感知

工业控制系统安全扩展	节点的管理和数据融合处理 室外控制设备防护、工业控制系统网络架构安全、拨号使用控制、无线使用控制和控制设备安全

资料来源：中商产业研究院，中信建投证券研究发展部

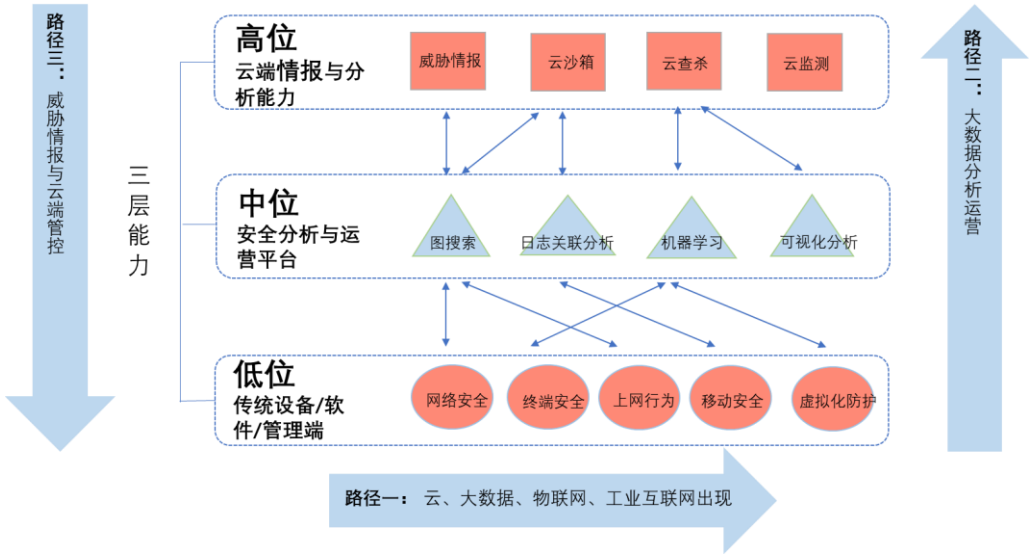
2.4 大数据驱动网络安全防护思想成为共识和主流，数据成为未来网络安全公司最重要资源

安全威胁潜伏越来越深，企业数据量越来越大，关联性越来越难发现，传统安全防护思路已然过时，大数据驱动网络安全防护成为共识。传统网络安全是哪痛医哪思路，找出潜在网络威胁需要分析企业数月各个设备的日志、流量，随着所采集和分析的数据量越大，越来越难发现各类数据关联、重构事件所需时间也越长。随着企业 IT 规模越大，储存与分析的安全信息越来越多，发现潜在威胁的难度也越来越大，传统地利用 SIEM 来处理大量的日志数据和情报数据收效甚微，甚至会陷入大量误报的漩涡中去。为改变这样的现状，奇安信提出必须坚持数据驱动安全理念，建设大数据驱动的态势感知和应急指挥平台，形成数据驱动的安全协同防御体系，帮助政企机构提升高级威胁和内部威胁的检测和防护能力。构建数据驱动安全体系必须要保证充足地数据源、拥有高中低三位一体的安全能力以及全方位态势感知的能力：

1) **保证充足的数据源。**对于规模化的企业，发生在自身设备与相关 IT 系统的数据交换与日志信息，给企业带来了大量的数据源。同时，利用网上公开的数据、产业上下游数据等外部数据的重要性也不容忽视，比如利用网上公开数据追踪 APT 组织的方法。分析数据分为以下几类，分别为系统、应用、存储、网络设备、业务、Agent 监控等等。其中最直接输出的价值便是威胁情报，威胁情报可以通过溯源来寻找攻击者，最主要的来源便是通过各类安全产品记录的数据进行提取与管理，如 EDR、IDS、IPS、Waf、流量审计、开源情报、日志审计。威胁情报已经成为驱动安全事件响应的核心，是安全设备、安全人员能力提升的关键要素，也是数据驱动网络安全核心要素之一。

2) **构建高、中、低三位一体的安全能力。**有了充足的数据源以后，就需要构建安全能力向数据转移的高、中、低三位一体安全能力模型。低位是我们长期以来信赖的网络安全基础软硬件，为用户提供基础的安全防护能力；中位是中流砥柱，关联分析、可视化、机器学习等大数据衍生的应用都在中位之列；高位能力的核心是云端的安全运营能力，包括了威胁情报、云端沙箱、云查杀等。低位就像四肢，负责具体行动的执行；中位就像心脏，负责为全身器官输送血液和能量；高位就像大脑，负责为中低位提供战略支撑。

图表32： 未来网络安全公司构建“高中低”三位一体能力极为重要



资料来源：奇安信，中信建投证券研究发展部

3) **全方位的态势感知。**最终需要全方位态势感知赋予企业真正的网络安全能力。而态势感知需要包含以下 5 个要点：第一，坚持业务导向，管理是根本，技术是支撑；第二，关口前移，从“查漏补缺”到“系统规划”；第三，拥有纯正的大数据基因，具备完善的大数据采集、大数据存储与计算、大数据治理、大数据建模与分析、大数据应用于大数据持续运营六大要素；第四，以人为核心的网络安全运营能力；第五，攻防兼备的应急响应能力。

4) **专业的安全数据人员：**无论是研判分析、追踪溯源、态势感知和威胁情报，都离不开人的分析和运营，大数据也增加了运营人员的智能，数据驱动安全的理念，不仅让设备更智能，也使得用大数据让分析研判和追踪溯源的人更智能，让安全一线运维的人更加智能，实现安全运行和维护的操作化。

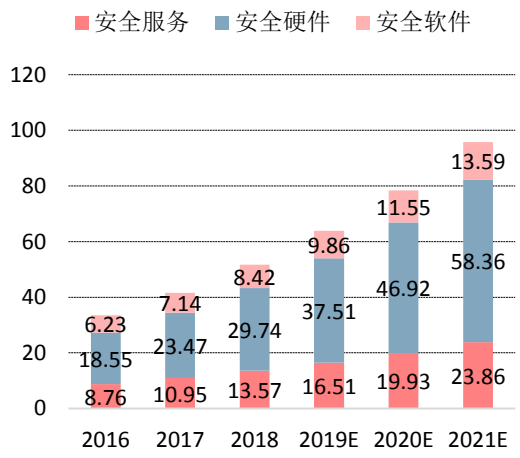
图表33： 大数据驱动人机协同安全运营

资料来源：奇安信，中信建投证券研究发展部

2.5 伴随新应用场景出现和积极防御类网络安全产品快速增长，安全运营服务市场增长迅速

我国安全服务市场空间广阔。在全球市场中，随着云安全和移动安全等新型领域安全的发展，安全服务化理念深入人心，安全服务成为发展热点，2017 年占整个信息产品市场的 61.8%。目前中国信息安全市场仍是以硬件为主，2017 年国内信息安全硬件市场占比最大，达到了 50.1%，安全服务只占整个信息产品市场的 11.2%。随着中国信息产业和网络技术的发展，传统的信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全行业必将向国际看齐，未来中国安全市场将由硬件为主转换为服务为主。目前国内信息安全领域的重要企业，均在开展行业解决方案策划和推广工作，从产品导向型企业向服务导向型企业转变，以适应未来用户定制化服务和细分市场等发展趋势。未来三年，随着云计算、大数据与智慧城市的快速发展，更多的大型企业趋向于定制化安全服务，安全服务市场将持续增长，基于软件及服务的安全产品市场将是下一个爆发点。根据赛迪顾问预估，2020 年安全服务市场规模将达到 108.6 亿元，未来三年复合增长率为 33.25%。安全服务又分为安全咨询、安全运营和安全集成三部分。

图表34： 中国网络安全市场规模，服务占比仍然很低（单位：亿美金）



资料来源：IDC，中信建投证券研究发展部

图表35： 根据中国信通院数据，在安全服务三个分类中，过去一年安全运营服务收入增速最快

资料来源：中国信通院，中信建投证券研究发展部

新时代发展安全运营服务是传统安全服务模式转型乃至整个网络安全建设的必经之路。在信息安全建设的先期，很多行业企业为满足信息安全基本的合规性要求，通过购买软硬件设备、设立岗位和部门，部署和管控系统，并进行日常维护。但是这种靠堆砌产品和服务以及简单粗略的管理，随着云物移大智等新技术的深度发展与融合，以及智能化手段的应用，安全环境发生了重大改观，系统日益复杂，业务规模不断扩大，业务关联性和架构复杂性、信息资产和数据总量成倍增加，加之网络防护边界日益模糊等因素，导致安全威胁随之陡然加大，过去还勉强可用的方法已然显得力不从心、难以为继。网络安全保障工作亟需迈上一个新的台阶，突破过去静态的、被动的、孤立的和局部的局限，以解决安全管理与技术安全协同不到位，不断优化及提高其安全能力，建立起持续运营的安全运营体系，从业务系统安全的角度出发，保障业务活动安全稳定。在此背景下安全运营开始逐渐兴起。**安全运营是一系列规则技术和应用的集合，目的是要构建整体联动的主动安全防御体系，围绕业务活动场景，实现预警响应处置恢复的闭环，充分使安全要素最优配置，动态地智能化地协同内外资源，保障组织核心业务平稳运行，并持续迭代优化，有效抵御内外部威胁。安全运营是促进网络安全良性发展，安全建设实际落地的必经之路。**

安全运营包括运维，但高于运维，可以说是传统安全建设的集中和升华。近年来，一些机构企业相继建立安全运营团队，一些安全企业也着手建立安全运营中心。**目前安全运营服务主要分为三种模式：**

1） **驻场运营服务**：以 360 企业安全态势感知解决方案的驻场运维人员为例，运维服务包括协助用户运维人员，从事 NGSOC 平台的日常告警处置、定期统计报告、流量分析、安全规则调优等工作，与后端产品专家和安全专家建立快速响应通道，能够做到事件的及时反馈与处理，提升安全运营工作效率。因此驻场运维人员必须有云端强大的信息安全专家团队作为支撑。

2） **城市安全运营中心**：以启明星辰推出的安全运营中心为例，运营中心的服务包括由专业安全团队进行全年不间断监测服务，可及时掌握网络现状及趋势，使企业做好预警、通报、处置等工作。实现对网络中各类海量网络数据的实时监测，对各类安全及情报的快速获取，通过专业安全团队，应用人工智能、大数据分析等技术，为用户可视化展现当前网络及业务系统的健康状态与未来走势，为各类业务系统建立可度量的风险模型，为用户提供事件分析与审计、风险评估与度量、预警与响应、安全态势分析等多项安全服务，并借助标准化的流程管理实现持续的安全运营。可以说从第三方独立视角，以“解决安全风险”为诉求，从管理、技术、制度、流程、人员等多方面进行优化及改进安全建设，从而实现业务动态安全的建设目标

3） **安全托管服务**：以亚信安全和深信服的安全托管服务为例，采取基于云安全监测技术的服务模式对客户网站进行全托管管理。客户仅需提供网站的域名和对应 IP 地址，无需在网站上进行任何代码的改动，也无需安装任何服务端 Agent，即可享受就 7×24 小时不间断的安全监测服务和安全专家的安全检测服务，并可定期获得一份专业的安全检测月度报告，作为向领导汇报、了解网站安全状况的有效途径。

“智慧城市”建设持续落地带来更多专业城市安全运营服务需求。2018 年我国智慧城市 IT 投资规模达到 4800 亿元，市场规模已接近 8 万亿元，未来 5 年将保持年均 33.38%的复合增长。智慧城市中存储了海量城市数据信息，涉及政务、医疗、社保、交通等行业，而智慧城市的核心之一便是数据的共享与融合，确保海量数据在融合与使用过程中居民个人隐私信息、企业和政府敏感数据不被入侵篡改和肆意泄露。因此需要有面向智慧城市的专业城市安全运营服务来确保智慧城市的运行安全。城市安全运营服务业务将开启新的安全服务市场，为相关企业带来新的利润增长点。

以态势感知平台为代表的在各行业的快速拓展下，安全运营服务需求快速增长。随着以态势感知平台、APT 防护为代表的主动防御类信息安全行业领导公司都纷纷推出网络安全运营驻场服务或者城市安全运营中心，帮助政府机关、企业进行专业的安全运维、数据分析支持，尤其是利用网络安全厂商大数据、AI 能力提供事件分析与审计并做好预警服务。普通客户因为不具备对海量网络安全相关数据的分析能力，因此未来随着政府和企业客户网络安全系统越来越复杂，获得数据也越来越复杂，对第三方运营服务需求也会逐步增加。

未来随着政企对主动安全防护、预测性防护需求的提升和信息安全系统复杂化，所需高级安全服务需求也会提升。除了做好基础设施的网络安全防护，随着信息安全预测性防护需求增加，如对抗式演习服务、基于威胁情报的预警响应服务和工业控制系统信息安全服务需求也会逐步增加。

三、党政军安全需求增长和新场景推动公司业务稳健增长，安全运营服务成为公司发展新动力

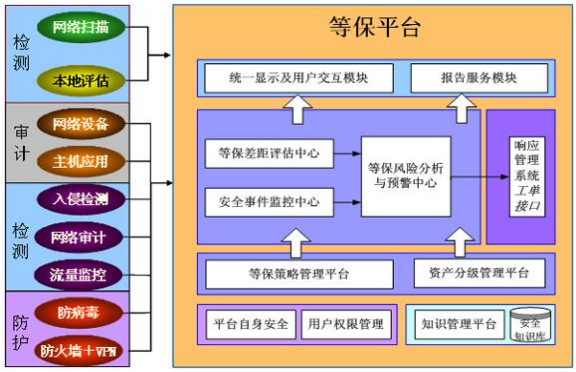
3.1 多重因素助力党政军行业网络安全需求加速增长，促进公司 2019~2020 年业绩加速

“十三五”规划接近尾声，军工政企单位订单需求高增长。启明星辰服务政府和众多央企行业客户，受益于未来安可自主可控增长。受到军改影响，2018 年公司军工订单不达预期影响了 2018 全年收入和利润增速。而今年距离国家十三五规划仅余最后两年，各级政企单位、军队均加大网络安全投入和建设，启明星辰集团各子公司及业务部门正在积极跟进。在 2019 年上半年军工领域的签单恢复正常，同比增长 35%，为所有领域最高，预计 19 年预计全年军工订单收入同比增长 40%—50%。在政府领域启明星辰为国家 100 多个部、委、办、局用户提供安全保障并服务电信、金融、能源、烟草等多领域大型央企，提供安全产品、服务和解决方案，党政军占公司收入占比超过 60%，市占率稳定（2018 年市占率约为 5.3%）。对包含党政军在内的多行业高端客户的网络安全需求理解和把握能力使公司长期在行业内赢得广泛认同，同时公司也能紧跟行业发展适时自研或者通过投资并购推出新产品、新业务，良好和完善体系化的营销体系优势、品牌优势和整体解决方案能力使公司成为多行业高端客户稳定合作伙伴。未来受益于安可和自主可控包含党政、电信、能源、金融等多行业在内重点客户采购需求增长，预计公司主要行业客户需求增速将加速。

图表36： 启明星辰泰合态势感知平台

资料来源：公司官网，中信建投证券研究发展部

图表37： 启明星辰基于等级保护的金融信息安全保障体系整体架构



资料来源：公司官网，中信建投证券研究发展部

等保 2.0 发布、HW 行动加速党政军未来两年网络安全产品采购需求，促进行业增长。2019 年 5 月，《网络安全等级保护制度 2.0 标准》正式发布，实施时间为 2019 年 12 月 1 日，等保 2.0 增加了新对象的安全防护如云计算平台、大数据平台、物联网系统、工业控制系统等，增加了对关键基础设施的防护如明确规定了轨道交通、电力能源等基础设施纳入保障范围，增加了对新产品和技术的要求，例如要实现态势感知，能够检测对重点节点及其入侵的行为，对各类安全事件进行识别报警和分析等等，因此未来新产品、新行业和新的防护对象都将促进网络安全行业市场规模持续保持快速增长。2019 年 HW 行动力度加大，覆盖范围增加且考核排名机制趋严，因此 2019 年 H1 HW 行动为全行业带来了超预期的服务和产品采购机遇，尤其对入侵检测、云安全、态势感知等产品带动作用明显，我们预计护网行动带来的产品订单有望在 2019 年下半年对公司收入产品推动。

公司利用自身安全大数据采集和分析优势，推出泰合态势感知平台，全面迎合军工、政企等对全天候态势感知解决方案需求，已经在多行业客户实践和应用。《“十三五”国家信息化规划》明确提出要加强网络安全

态势感知、监测预警和应急处置能力建设，特别是对于军工、党政等行业来说,其核心网络及重要业务系统的安全稳定，关系着国计民生及国防安全,容不得半分懈怠，态势感知能力的建设，可以有效整合分散在行业用户信息网络环境中的各类信息要素。在布局、实践态势感知方面，公司运用安全大数据为基础，结合全球领先的数据采集能力，全面支持资产采集、流采集、文件采集、包采集、漏洞采集、情报采集等能力，对设备、主机、日志、进程、服务等全要素信息的归并，利用公司专长的安全大数据分析经验，帮助用户构造全方位、全天候态势感知系统的建设需求。具体来说，可为用户提升网络态势监控、威胁分析、日常运维、事件处置等安全能力建设水平，在网络新常态下，实现诸如：网站整体运行态势监控、暴露或内部资产识别监控、内外部入侵行为定位、行为分析建模、高级持续威胁判定、失陷主机态势分布、政企侧漏洞闭环管理、攻击链还原、威胁情报管理、终端管控等高价值业务和场景的管理能力。公司以增强型分析能力为交付物的**泰合态势感知平台**，已在国内多个行业用户实践和运用。

3.2 “云大物移”新应用场景和新解决方案为公司提供中长期发展动力

公司在物联网安全（工控安全）、云安全以及轨交、能源等新增基础设施行业不断拓展新产品和解决方案，2018 年公司三大战略新业务（智慧城市安全运营、工业互联网安全、云安全）的业绩初现规模，实现销售约 4 亿元，确认收入超过 2 亿元，新场景和新行业解决方案将为公司提供中长期发展动力：

以专有云/私有云安全解决方案为核心，公司不断完善云端安全方案。由于深入参与政务云和智慧城市建设，云安全综合解决方案集软件定义安全、安全资源虚拟化、安全能力融合、云安全监管服务为一体的综合型云安全交付架构，提供不断完善的专有云/政务云安全产品，产品包含：安全监测子平台、态势感知子平台、安全应急子平台、安全事件处置子平台、安全防护子平台等。公司利用独特的开放性与兼容性，帮助用户在各种云的环境下构建其纵深防御安全体系，适合为私有云运营者构建整体安全解决方案。

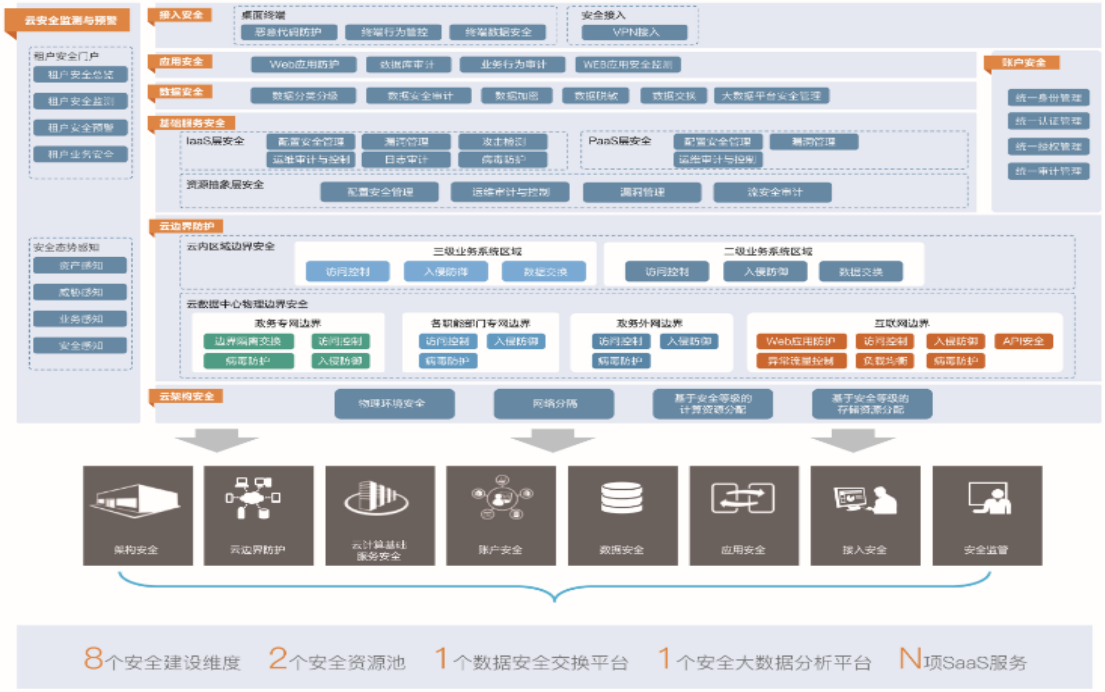
图表38： 公司云安全产品

云安全产品	产品介绍	技术优势
云子可信 SaaS	云子可信是启明星辰自主研发的一款面向中小微企业的终端安全 SaaS 云平台。该平台专注于提供 IT 管理和 IT 安全服务， 提供全套专业的解决方案，满足于不同的企业的管理需求。	云屏蔽；高效的升级方式；终端安全管理能力强大；良好的用户体验
云安全资源池	云海安全专有云系统是启明星辰针对私有云或虚拟化资源池用户推出的，新一代安全安全资源池平台型产品。产品可充分满足用户对虚拟化环境的深度防护和弹性扩展等需求。	动态自适应安全；方案适用性强；安全独立运营
云 Web 应用审计	天玥云 web 应用审计专门适用于云环境下的数据库审计及防护产品，可兼容主流云平台，产品着重对应用系统操作流程进行梳理，发现流程中的异常操作，提供页面仿真回放功能；根据应用系统中的操作数据智能发现越权行为，对敏感数据模糊化结果进行核查；Web 应用审计产品对应用系统中的疑似攻击、弱口令、性能瓶颈都具有监测能力。	易于扩展的分析条件；基于场景的审计；灵活的规则定义能力；加密协议审计能力；云环境的全面支持
云数据库审计	天玥云数据库审计专门适用于云环境下的数据库审计及防护产品，可兼容主流云平台，实现对云环境中数据库操作的实时审计及防护。	灵活的规则定义能力；全面的协议覆盖能力
云安全管理平台	启明星辰泰合云安全管理系统 TSOC-USM-CSM（简称“泰合 CloudSOC”）秉承了启明星辰泰合本部一贯扎实领先的管理平台品质，面向云计算特点和用户使用场景进行功能开发而打造的一款云中安全管理平台系统产品	威胁情报利用；多租户视角；资源池数据隔离；组件化部署；云安全可视化；云安全合规

资料来源：公司官网，中信建投证券研究发展部

公司利用在传统 IT 安全领域的技术积累，通过改进技术适应云构架，基本实现了在云安全领域的产品全覆盖。2018 年，公司推出新一代云安全资源池，加强对云管端纵深防御体系的建设，防护云环境及虚拟化资源安全，实现对各种云平台包括华为云、腾讯云、浪潮云、天翼云、联通沃云等及其云租户业务的安全监测、防护、响应及预警能力。此外，公司积极推进、参与云计算产业生态合作，2018 年加入华为安全商业联盟，成为华为首批终端安全奖励计划合作伙伴；与中国电信天翼云携手，共同发起成立“天翼云安全生态联盟”，为天翼云打造符合业务需求的云安全运营体系，为中国电信从 IT 及 ICT 向 DICT 转型提供助力。云子可信是公司自主研发的面向中小微企业的企业终端安全云平台，目前已有全国各地的 10000 多家企业正在使用。

图表39： 启明星辰云安全解决方案



资料来源：公司官网，中信建投证券研究发展部

启明星辰在工业互联网领域多产品和整体解决方案处于领导地位，多年一线工控安全保障经验以及前沿物联网深度安全技术研究使公司具有丰富经验。早在 2010 年伊朗震网病毒事件发生后，公司就将工控安全作为一个重要方向进行深入安全研究，2014 年成立贯穿前中后场的工控安全部，开展全集团的工业物联网信息安全业务。经过在电力、石油化工、先进制造、轨道交通、烟草等多个行业的广泛应用和打磨，启明星辰的工业防火墙、工控异常监测与审计、工控隔离设备、工控漏洞扫描、工控安全管理平台等多款产品已不断深度完善，基本夯实了已有技术的工业协议深度防护、异常流量自学习、关键设备运维审计、工控隔离交换、工控漏洞挖掘等多项核心技术，且与各行业应用场景无缝联接，产品能力在行业内处于第一梯队。截止目前，自主原创发现的相关物联网和工控系统的漏洞近 200 个。公司工控安全业务发展速度较快，目前在全国排名第一，预计 2019 年有望增长 50%以上。

图表40： 公司工控安全产品

工控安全产品	产品介绍	技术优势
工控 IDS 与审计	天阗工控异常检测系统是启明星辰集团面向工业企业领域客户推出的针对工业	强大的扩展检测定义语言；网络伪造报

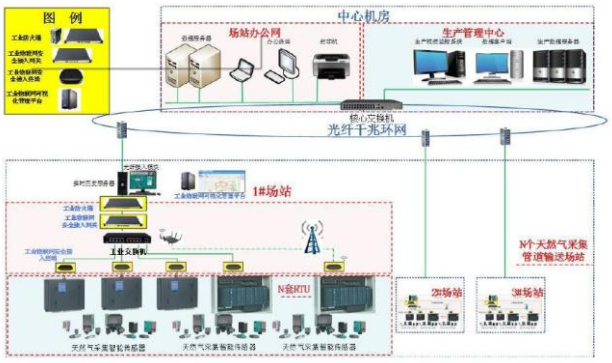
工控安全产品	产品介绍	技术优势
	控制系统的专用网络安全检测系统。该产品拥有国内顶尖的入侵检测技术，支持对多种工业控制网络协议的深入解读，提供特有的工控网络安全检测策略。	文攻击检测；工控网络特有检测策略；特征事件覆盖全面
工控脆弱性扫描	天镜脆弱性扫描与管理系统 V6.0-工控系统专用版根据工业控制系统已知的安全漏洞特征，对 SCADA、DCS 系统、PLC 等工业控制系统中的控制设备、应用或系统进行扫描、识别，检测工业控制系统存在漏洞并生成相应的报告。	可视化的工控系统安全风险展示；全面的工控系统漏洞扫描能力；准确的工控系统信息发现能力
工控检查工具箱	天镜工控系统安全检查工具箱是一款按照等级保护基本要求为依据，通过管理制度访谈和技术工具检测手段相结合，实现对工业工控系统安全进行等级保护合规性风险评估的便携式一体化设备。	集专业性与先进性于一体；良好的规范性和扩展性；多维度多样化的数据分析展示；便携性、易用性
工控态势感知	启明星辰工业态势感知系统定位于为用户实现态势感知能力的上层平台，该平台为基于大数据架构的海量信息采集与处理型系统。平台系统分层次提供了海量安全信息的采集、存储、集中分析和综合态势呈现功能。	工控网络协议的深度识别；流安全检测与分析技术；多维度的网络流行为可视化分析；多方位安全态势感知
工业防火墙	天清汉马工业防火墙 IFW-3000 系列是为工控网络安全专门设计的防火墙产品。具备军工级硬件品质，采用宽温、防尘、抗电磁、抗震设计；提供导轨式、机架式两种形态；支持 BYPASS、热备机制、接口联动、端口冗余多种技术，全方位保证设备可靠运行。	协议内容自定义过滤；工业威胁专业防护；未预置工业协议自由定义；工业协议内容细粒度检测；工业协议全面支持

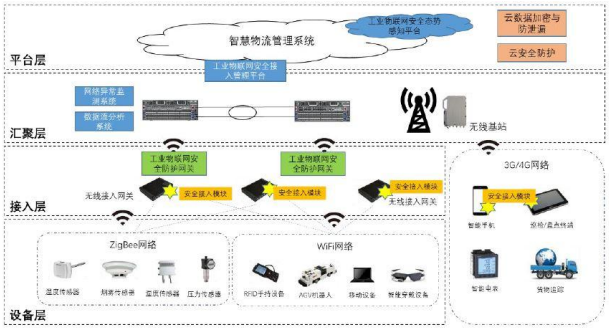
资料来源：公司官网，中信建投证券研究发展部

公司深耕电力、石油化工、先进制造、轨道交通、烟草、燃气等多行业工业网络安全解决方案。过去几年公司已在多个行业根据行业业务特点沉淀出切实可行的安全解决方案，在所属行业内产生了标杆示范效应。1）**石油行业，**已开展多个油田、炼化厂两网隔离，实现注、采、输从井口到场站各类地面设备运行状况、设施工艺参数等数据安全传输到数据中心；**2）电力行业，**主要针对各级调度的电力监控系统、智能变电站、用采系统、电厂生产控制系统、电网配网的安全防护。参照 36 号文要求，公司已有多个电力工控系统的防护案例，实现了工控网络入侵检测、敏感指令检测、异常流量监测，工控系统边界安全防护，运维操作审计，操作站安全管理等安全技术建设；**3）轨道交通行业，**综合监控系统和信号系统均有多个建设样板工程，重点解决了对车站级到中央级的严格访问控制，车地之间、自动化系统之间的安全通信，自动发现网络中的活跃主机、端口，以及接口间的访问关系，对工控网络的各种入侵、病毒、木马攻击行为，发现 PSCADA、BAS 等系统指令异常，统一实时监测安全状态；4）烟草行业，公司作为烟草行业工控安全标准制定参与者，扎实走稳每一步，已落实卷烟厂、复烤厂、醋纤公司、商业公司物流系统等众多工控安全项目；先进制造行业，针对机床类的精密加工场景，重点解决其普遍存在的网络无安全域划分、机床近端防护措施缺失、运维操作无审计纪录、缺少违规异常发现机制等问题。

图表41： 公司油气开采物联网系统安全防护解决方案示意图

图表42： 公司智能仓储智能安全防护解决方案示意图



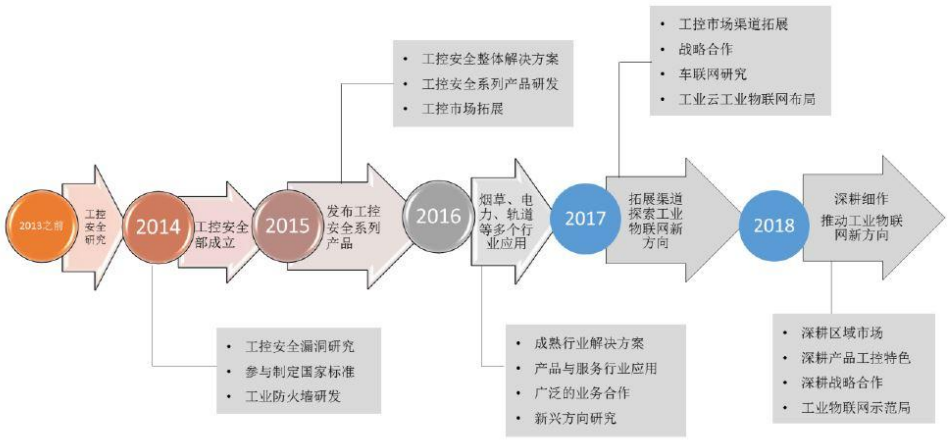


资料来源：公司官网，中信建投证券研究发展部

资料来源：公司官网，中信建投证券研究发展部

城市轨道交通、电力等基础设施行业安全市场潜力巨大且增长速度较快，公司在轨道交通安全领域布局尤为领先。《网络安全法》规定“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”以轨道交通行业为例，城市地铁的信号系统、综合监控系统、自动售检票系统等均需要部署网络安全防护系统，新规划的城市地铁就要将网络安全纳入到信息系统总体规划中，同时要求对于“关键信息基础设施的运行安全”从保护制度、职责分工、安全要求、统筹协调机制等方面作出了详尽的规定。我们预计未来五年城市轨道交通等基础设施行业工业控制安全将成为信息安全行业拓展潜力最大的下游行业。公司是轨道交通领域网络安全建设先行者，公司针对城市地铁网络安全存在的痛点，提出了不同的解决方案，通过对轨道交通多年的研究，已经为北京、上海、深圳、成都、广州等城市地铁建设提供了网络安全服务，目前与 80%以上已开通地铁城市建立了合作关系，通过 100 多个安全项目形成了独有的行业认识与经验，轨道交通安全业务增速 2019 年预计保持在 50%以上。

图表43： 公司工控安全发展历史



资料来源：公司官网，中信建投证券研究发展部

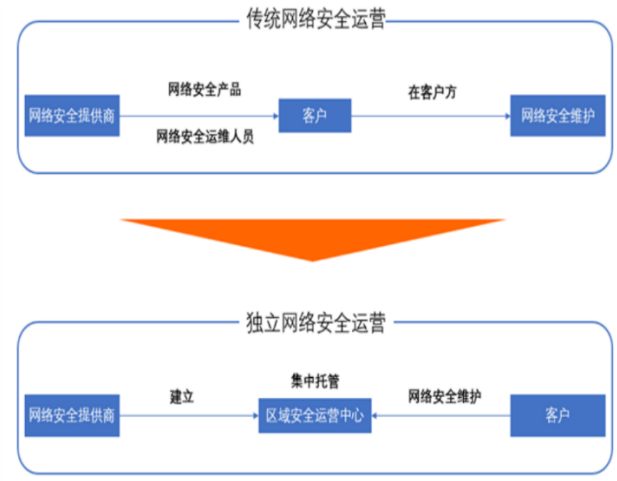
图表44： 启明星辰城轨云网络安全解决方案

资料来源：公司官网、中信建投研究发展部

3.3 首提第三方独立运营，城市安全运营服务中心业务将促进公司智慧城市大数据发展，为公司提供长期发展动力

中国安全服务市场高速增长，城市安全运营业务是公司未来长期战略重点方向，将为公司带来大量智慧城市相关安全数据，为公司长期发展提供优势。智慧城市中存储了海量城市数据信息，涉及政务、医疗、社保、交通等行业，而智慧城市的核心之一便是数据的共享与融合，确保海量数据在融合与使用过程中居民个人隐私信息、企业和政府敏感数据不被入侵篡改和肆意泄露。因此需要有面向智慧城市的专业安全运营服务来确保智慧城市的运行安全。**作为国内网络安全领军企业，启明星辰走在智慧城市安全建设队伍的前沿，战略布局城市级安全运营中心，为智慧城市健康运营提供强力的网络安全事件防御能力。安全运营具体内容包括：**1）围绕业务系统进行日常安全监测，做好随时发现问题的准备；2）如有问题，找到问题并分析原因，定制方案进行解决；3）通过持续运营方式（人员、流程，工具，平台等等）；3）定期查看指标是否达成目标。

图表45： 公司提出网络安全行业运营新趋势



资料来源：公司公告，中信建投证券研究发展部

图表46： 公司提出的评价安全运营的 5P 核心要素

资料来源：公司官网，中信建投证券研究发展部

2016 年开始启明星辰已全国范围布局智慧城市的独立安全运营中心建设，首次提出了以“第三方独立安全运营”作为保障网络安全的重要手段，战略布局城市级安全运营中心，为智慧城市健康运营提供强力的网络安全事件防御能力。2017 年 12 月，国内规模最大、最具专业实力的企业级安全运营中心——启明星辰北斗成都安全运营中心正式启动，成都安全运营中心是启明星辰集团打造的首个北斗安全运营中心，也是目前全国首屈一指的安全运营中心，占地约 800 平米。**未来城市安全运营中心一方面将为公司带来海量各领域安全数据，为公司积累城市安全大数据，促进公司长期的数据安全分析能力提升和产品研究能力提升；一方面城市运营中心也将增加公司与当地客户的粘性，通过发现当地客户基础设施和网络中存在的安全漏洞和问题，给客户提供更完善的解决方案，为公司带来安全解决方案或者安全产品订单。**

图表47： 启明星辰提出网络安全运营 5P 核心要素

要素	核心内容
Policy 安全策略	安全策略可被视为安全治理的“宪法”，它们必须明确地与组织的战略安全目标保持一致，并为实现这些目标提供支持。良好的安全策略是组织战略的一部分。安全运营常说的以业务为核心，以安全能力作为交付即是安全策略的一种体现。
Product 安全产品	安全产品是指用于协助安全运营平台进数据采集，以及保障安全运营平台网络架构的合理及安全性的产品。安全产品一般分为监测工具和网络及安全产品，其中监测工具用于安全数据的采集，网络及安全产品用于对安全运营架构进行保障。
Platform 安全运营平台	安全运营平台主要有两个作用，一方面用于对运营对象的安全进行整体监控和态势感知，预知风险，通过可视化展示，直观地呈现运营对象的安全现状及威胁，同时通过 7*24 小时持续监测，使安全从静态向动态转变，掌握主动权，更好的进行风险管理和安全决策。另一方面，基于用户所采购的安全服务和安全运营流程，提供统一的安全运营服务管理平台。 安全运营平台一般需要具备数据采集、数据存储、数据分析、API、可视化展示等功能。通过采集系统，采集各类安全数据，对数据实现整体采集与清洗，构建数据资源池，为分析系统提供数据基础；分析系统利用云计算、大数据等技术，结合各类先进的安全算法，通过机器学习，关联分析和深度分析等，结合安全核心数据库，对安全数据进行分析和处理；通过 API 接口进行数据共享，同时为对外共享和向内接入提供安全接口和通道；最后，对所关注的数据进行综合呈现。
Professional 安全专业人员	安全运营人员根据安全运营的场景，可以按照不同的维度进行人员划分，常见的有三种划分方式： 第一种划分方式：一级分析师、二级分析师和三级分析师，根据能力模型直接按照层级划分，此为国际主流的划分方式； 第二种划分方式：安全监测人员、安全分析人员、安全响应人员和安全运维人员，根据功能进行划分，可以实现运营流程的

要素	核心内容
Process 流程	闭环； 第三种划分方式：网络安全专业人员、主机安全专业人员、数据安全专业人员等，根据专业能力进行划分，能更好地针对具体的场景进行安全运营。 流程是经过清晰定义用于完成特定任务的所有必要步骤，在长期的安全运营过程中，需要根据实际场景制定不同的安全运营流程，以保障安全运营的规范和有效。 流程一般分为内部流程和外部流程。内部流程主要是组织内部安全运营所需的流程，主要包括业务流程、操作流程、分析流程和技术流程等；外部流程主要是来自监管单位、主管单位和其他第三方的安全要求或安全事件处置所要求的流程。

资料来源：中信建投证券研究发展部

作为集团公司的战略新业务，全国范围内城市安全运营业务的开展在 2018 年取得了良好的效果，预计 2019~2020 年仍然较保持高速增长。2018 年公司实现安全运营中心业务订单 1.5 亿，收入 0.5 亿元。从安全运营中心的业务形式来看，城市安全运营中心订单平均签订 3 年，每年确认 1/3 收入，未来能够创造持续性的收入。针对 2018 年底前已建成的安全运营中心，2019 年上半年基本完成基础建设并完成团队组建，开始正式运营且运营情况良好，2019 年上半年新增运营业务订单过亿元。按照公司的增长目标，安全运营中心业务 2019 年、2020 年有望分别实现 200%和 100%的增速，对应 1.5 亿元、3 亿元收入规模。目前，全国运营体系已基本形成北京、成都、广州、杭州四个运营业务支撑中心及二十余个城市级运营中心，并已形成成熟的标准化运营体系，未来在持续扩大已有运营中心业务的基础上，运营中心业务将向其他二三级城市拓展，目标 35 个运营中心。

城市安全运营中心业务将推动公司中期业务增长。根据公司公告安全运营中心前期综合毛利率约 30%-40%，后续约能达到 40%-50%的水平。由于城市安全运营中心建设期较长，目前正处于“跑马圈地”阶段，后续随着业务量的增长，盈利能力有望逐步改善。2017 年 11 月，公司公开发行可转换公司债券募集资金，主要用于济南、杭州、昆明、郑州安全运营中心的建设，主要包括：安全检测中心、安全应急中心、安全研究中心、咨询服务中心、终端防护中心等的投建。拟投入募集资金 104,500 万元，项目全部达成后，预计四地带来年均净利润为 2,122.17 万元、6,282.96 万元、13,241.99 万元、14,659.69 万元。

图表48： 公司已经签署和运营的安全运营中心

主要安全运营中心	项目进展	介绍
成都安全运营中心	2017 年 12 月启动运营	成都安全运营中心以智慧城市的相关应用为研究主体，由专业安全团队进行全年不间断监测服务，可及时掌握网络现状及趋势，做好预警、通报、处置等工作。
青海安全运营中心	2018 年 11 月投入运营	全国首个省级安全运营中心，是青海省深入实施“五四战略”和“一优两高”战略，从更高站位、更大格局、更宽视野推动青海网络安全和信息化工作更好融入国家战略的阶段性成果。
青岛安全运营中心	2018 年 11 月签署	继北斗（济南）安全运营中心后的启明星辰集团在山东省内落成的第二个安全运营中心，是集团安全运营业务向胶东区域、保密领域的拓展的重要一步。
天津安全运营中心	2018 年 5 月签署	以天津为中心辐射京津冀地区的智慧城市安全独立运营中心，遵循“安全先行”、“秩序可控”的原则和目标，积极参与天津市智慧城市建设运营工作，提升天津市网络安全技术体系综合能力。
广州安全运营中心	2017 年 11 月签署	由国家信息中心、工信部、两院院士及国内新型智慧城市建设领域的权威专家、政府领导参与并主持的新型智慧城市建设专家座谈会，并在会上发起成立港澳大湾区新型智慧城市产业联盟。启明星辰作为发起单位之一
昆明安全运营中心	2017 年 5 月签署	启明星辰西南区域总部基地项目建成后采取“政、产、学、研、资、用”相结合的产业体系和技术创新服务体系，建设昆明智慧城市安全运营中心和网络空间安全学院
郑州安全运营中心	2017 年 9 月签署	以“平台+服务”式的新安全运营方式，为客户提供持续的、及时的、定制化的安全服务，为智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应

主要安全运营中心	项目进展	介绍
	急处置机制	

资料来源：公司公告，中信建投证券研究发展部

3.4 持续投资并购建设不断完善的网络安全生态，在网络安全技术快速迭代和创新中保持领导地位

党政军和央企网络安全市场整体规划能力和解决方案能力越来越重要，公司持续通过投资并购建设网络安全生态。我们不断强调在网络安全下游行业快速发展、新产品叠出的时代，网络安全公司生态体系建设的重要性。中国市场大型客户比较注重网络安全整体解决方案，要求承建网络安全项目的供应商具备整体规划能力和比较完善的产品体系。而随着云计算、物联网的快速发展，因此网络安全龙头公司除了自主研发产品外，毕竟通过公司自身投入研发精力和人力有限，不能覆盖碎片化的网络安全场景和新产品，因此通过投资并购能有效弥补整体解决方案的不足。近年公司一直通过并购和投资手段建设自己的网络安全生态，储备未来网络安全发展关键技术和巩固细分行业优势地位。2019 年 H1 并购公司网御星云、赛博兴安均有较高增长，其中赛博兴安受益于军工行业采购回暖，为公司带来较大军工订单，除军工外网御星云也受益于政府在安可上的采购和 HW 行动带来的增长，2019H1 营收同比增长达到 38.72%。公司持股 13.68%的恒安嘉兴是具有“云—网—边—端”整体解决方案的通信网安全领军企业，弥补启明星辰在通信安全领域的短板。

公司在数据安全、工控安全、车联网安全、云安全等新兴领域均有领先投资布局。公司在近年发展较快的数据安全、工控安全、车联网、终端杀毒安全等领域均有领先的投资布局，目前公司独立完成 200+工控系统\物联网设备安全漏洞研究，参与等保 2.0 等十几项工控网络安全标准制定，融合防护、检测、监管的工业互联网安全运营中心。除了未来网络安全技术，公司也通过投资并购进入新的行业和领域，如之前通过赛博兴安补充军工资源和拓展空军类型客户。今年一月，公司增资易捷思达，将公司在信息安全技术及市场资源方面的优势与易捷思达在云计算及超融合领域的优势相互融合，达成强强联合、优势互补的目的，积极布局云安全业务。

图表49： 启明星辰并购或投资公司

公司	持股比例	主营业务	营业收入（元）	净利润（元）
赛博兴安	90%	网络传输加密、加密认证及数据安全、军队军工行业安全管控、不同安全域间网络互联等领域	168,249,774.71	59,003,440.09
四川赛贝卡	100%	数据库审计、运维审计和 4A 等领域	未披露	未披露
合众数据	100%	大数据分析及大数据安全领域，提供安全数据交换、网络边界接入、大数据分析处理与应用开发等方面的产品及解决方案	未披露	未披露
恒安嘉兴	13.68%	通信网安全领军企业，专注于网络空间安全综合治理领域，主营业务是向电信运营商、安全主管部门等政企客户提供基于互联网和通信网的网络信息安全综合解决方案及服务	488,302,535.41	18,371,842.00
深圳大成天下	23.81%	专注信息防泄密（DLP，DataLossPrevention）领域，近期推出了“72 小时”与“小密圈”等移动互联网云产品	20,162,938.45	-4,035,189.34
辰信领创	49.50%	病毒及恶意代码防范技术产品，实现从终端到云端的完整的、全方位的、立体化的安全防护体系	未披露	未披露
北京太一星辰	38.22%	专注于提供专业应用交付及高性能安全产品的技术性高科技企业。	26,179,470.73	6,261,346.34
SK Spruce	4.99%	WIFI、3G/4G 网络安全以及企业级移动互联安全解决方案。		

长沙智为信息	30.00%	以拒绝服务及洪水攻击防御为方向，面向政府、金融、企业、小型数据中心和 ICP 服务商推出的企业级专业 DDoS 防御系统	7,794,496.33	-845,000.32
易捷思达	5.86%	立于 2014 年 2 月，由 IBM 中国研发中心 OpenStack 核心研发团队创建，基于 OpenStack、Ceph、Kubernetes，Docker 等一系列开源软件为企业级客户提供云计算产品与服务。	未披露	未披露
上海安言	25.00%	专注于信息安全及 IT 风险管理咨询服务，为包括银行、电力、运营商和全球 500 强在内的百家以上重点企业客户提供各类适应其业务发展需要的信息安全及 IT 风险管理落地解决方案。	10,729,084.73	153,325.52
上海安阖在创	22.50%	由安在新媒体、黑客密室、安在影视，以及泛黑客文化 IP 服务四块业务构成。还拥有旨在为创业者提供交流分享服务的“安创汇”。	2,285,631.06	446,917.46
三门峡崤云	49.00%	主要为三门峡建设新型智慧城市提供互联网信息网络安全	114,830.84	-341,633.76
网御星云	100%	防火墙及 UTM 产品线等网络安全防护产品，WAF Web 防火墙等应用与数据安全防护产品，IDS 入侵检测系统等全网安全管理系列产品。主要为能源、烟草、金融行业提供服务	784,366,700	127,571,600
书生电子	100%	数据安全领域、数字签名、电子印章、电子公文		17,850,100
川陀大匠	100%	拥有计算机科学与技术方面的深厚背景，覆盖 Linux 内核开发，机器学习和算法设计等诸多领域。	未披露	未披露
优逸科技	12.28%	互联网账号保护服务提供商，为金融行业、电子政务、网络游戏、电子商务等提供专业的身份认证产品和解决方案。	未披露	未披露
攀克网络	10.72%	ASIC 专用芯片设计，VPN 硬件加密、网闸物理隔离、网络加速	未披露	未披露
数字冰雹	2.73%	大数据可视化展现	未披露	未披露
杭州磐联	10%	物流信息防伪	未披露	未披露
国保金泰	8%	安全隔离与信息交换系列产品	未披露	未披露
永信至诚	4.76%	网络安全产品、安全服务工具	未披露	未披露
方物软件	4.17%	自主研发的虚拟化软件	未披露	未披露
国信天辰	50%	提供信息安全规划服务等产品化服务、等级保护合规性咨询等合规性服务、信息系统安全运维等客户化服务，帮助企业实现组织信息安全体系的 PDCA（计划、实施、检查、改进）循环。	未披露	未披露
泰然神州	22.22%	虚拟化与移动安全，包括应用交付平台、安全堡垒机、运维审计系统、安全桌面等产品线以及电力、海关、电信、金融、公安安全解决方案	未披露	未披露
联信摩贝	17.59%	移动威胁防御、移动设备、应用、内容管控等移动安全产品和服务提供商	未披露	未披露
时代亿宝	3.49%	以声纹识别为代表的多因子认证技术及智能服务提供商	未披露	未披露
中海纪元	6%	智慧政务、智慧教育、智慧住建等 IT 解决方案	未披露	未披露

资料来源：Wind，公司官网，企查查，中信建投研究发展部

四、盈利预测与投资建议

伴随行业政策、技术革新和新场景需求，2019~2021 年进入网络安全行业高景气周期，2019~2023 年行业复合增速超过 25%，行业龙头显著受益。“云大物移”新场景驱动下防护对象改变，企业网络边界逐渐消失，政府和企业网络安全防护理念发生较大变化，网络安全不再是“补丁”模式，而是与信息系统建设同时规划，促进信息安全占 IT 支出占比逐步从 2%提升至 5%以上。2019 年 5 月，《网络安全等级保护制度 2.0 标准》正式发布，实施时间为 2019 年 12 月 1 日，等保 2.0 增加了新对象的安全防护如云计算平台、大数据平台、物联网系统、工业控制系统等，增加了对关键基础设施的防护如明确规定了轨道交通、电力能源等基础设施纳入保障范围，增加了对新产品和技术的要求，例如要实现态势感知，能够检测对重点节点及其入侵的行为，对各类安全事件进行识别报警和分析等等，因此未来新产品、新行业和新的防护对象都将促进网络安全行业市场规模持续保持快速增长。因此我们看到公司作为龙头厂商，近年在轨交、医疗、工控安全等领域增长迅速。2019 年 HW 行动力度加大，由于 2019 年 HW 行动覆盖范围增加且考核排名机制趋严，因此 2019 年护网行动为全行业带来了超预期的服务和产品采购机遇，尤其对入侵检测、云安全、态势感知等产品带动作用明显。2019 年预计中国网络安全市场规模将达到 602 亿， IDC 预计 2018~2020 年中国网络安全市场年复合增速将超过 25%，网络安全行业迎来了发展的黄金年代。我们预计未来，各业务线收入预测如下：

1）安全网关和安全检测业务：2016-2018 年，受军队行业下游影响，安全网关收入增速逐年下降，尤其 2018 受军改影响，军工订单不达预期，影响全年收入增速。2019H1 军工订单恢复正常，安全网关收入同比增长 11.17%，全年公司军工订单有望实现同比 30%~50%增长，将保证未来安全网关、安全监测业务的收入增长。2019HW 行动对安全检测类产品有促进作用。

2）数据安全与平台业务：2016-2018 年，公司数据安全与平台业务增速较快，其中 SOC、数据安全产品等在国内市场占有率处于首位，是公司增长速度最快的产品线，除了传统党政军市场需求逐步释放，在工业互联网、城市运营中心等业务对数据安全与平台业务需求也逐步放大，预计未来该产品线在公司收入中占比也将逐步扩大，预计 2019-2021 年安全网关收入增速分别为 32%、33%。

3）安全服务与工具业务：未来三年随着云计算、大数据与智慧城市的快速发展，大型企业趋向于定制化安全服务，安全服务市场将持续增长， 2020 年安全服务市场规模将达到 108.6 亿元，未来三年安全服务市场复合增长率为 33.25%。随着公司安全服务项目的逐渐落地，公司未来安全服务收入有望维持较高增长。

4）硬件及其他：由于公司进入新的高端行业和高端客户，整体集成项目大小逐步扩大，因此硬件及其他产品收入增速较快，2018 年以来公司硬件及其他收入增长较快，2019H1 同比增长 58.30%，预计 2019-2021 年硬件及其他收入将继续保持高速增长。

图表50： 公司分业务预测

分类	2016A	2017A	2018A	2019E	2020E	2021E
安全网关收入（亿元）	6.24	6.87	6.02	6.98	8.17	8.99
同比增速	*24.52%*	*10.21%*	*-12.37%*	16.00%	17.00%	10.00%
安全检测收入（亿元）	4.27	4.93	5.53	6.74	8.09	9.14
同比增速	*20.10%*	*15.37%*	*12.10%*	22.00%	20.00%	13.00%
数据安全平台收入（亿元）	3.69	4.81	6.1	8.05	10.71	12.85

分类	2016A	2017A	2018A	2019E	2020E	2021E
同比增速	*148.70%*	*30.28%*	*26.88%*	32.00%	33.00%	20.00%
安全服务和工具收入（亿元）	3.06	3.84	4.27	5.51	6.95	7.85
同比增速	*128.44%*	*25.54%*	*11.28%*	29.00%	26.00%	13.00%
硬件和其他收入（亿元）	1.79	2.12	3.06	3.98	5.25	5.93
同比增速	*-7.38%*	*18.47%*	*43.97%*	30.00%	32.00%	13.00%
其他业务收入（亿元）	0.22	0.21	0.24	0.23	0.23	0.23
同比增速	*11.99%*	*-5.44%*	*12.80%*	-2.99%	0.00%	0.00%
营业收入合计	**19.27**	**22.79**	**25.22**	**31.50**	**39.40**	**45.00**
营收同比增速	**25.65%**	**18.22%**	**10.68%**	**24.91%**	**25.08%**	**14.20%**
毛利率（%）	**66.81%**	**65.18%**	**65.47%**	**66.67%**	**66.31%**	**66.70%**

资料来源：Wind，中信建投证券研究发展部

投资建议：随着我国信息化程度提升，云大物移快速发展，国际局势紧张，国家对网络安全重视程度逐步提升，政策和需求共同驱动网络安全行业进入高景气周期，网络安全在 IT 开支占比也将逐步提升，2019~2023 年中国网络安全行业复合增速将达到 25%。2019 年行业迎来多重利好，军工订单恢复，安可进入正式实施阶段，促进公司营收和利润增速加速。作为国内网络安全领军企业，启明星辰走在智慧城市安全运营中心建设前沿，增强公司大数据能力和利用运营促进解决方案销售，安全服务获得快速增长。同时公司通过投资并购建立起的生态优势逐步体现，在新领域、新行业拓展速度较快，长期增长动力充足，我们预计 2019~2020 年公司归母净利润 6.59 亿元、8.31 亿元，给与“买入”评级。

五、风险提示

并购整合不达预期导致公司管理存在风险；

网络安全行业高端人才竞争激烈导致公司自身创新发展放缓风险；

行业内央企背景网络安全公司数量增加导致竞争加剧风险

分析师介绍

石泽薇：计算机行业首席分析师，执业证书编号：S1440517030001。香港中文大学电子工程硕士，专注于金融科技、信息安全、云计算、人工智能等领域的研究，2017 年初加入中信建投证券。2017 年《新财富》、2017~2018《水晶球》、2017~2018 年 wind 最佳分析师通信第一名团队成员。

侯子超：计算机行业分析师，上海交通大学软件工程学士、金融学硕士，专注于人工智能、云计算、互联网医疗、信息安全等领域研究。

研究服务

保险组

张博 010-85130905 zhangbo@csc.com.cn

郭洁 -85130212 guojie@csc.com.cn

郭畅 010-65608482 guochang@csc.com.cn

张勇 010-86451312 zhangyongzgs@csc.com.cn

高思雨 010-8513-0491 gaosiyu@csc.com.cn

张宇 010-86451497 zhangyuyf@csc.com.cn

北京公募组

朱燕 85156403- zhuyan@csc.com.cn

任师蕙 010-85159274 renshihui@csc.com.cn

黄杉 010-85156350 huangshan@csc.com.cn

杨济谦 010-86451442 yangjiqian@csc.com.cn

杨洁 010-86451428 yangjiezgs@csc.com.cn

社保组

吴桑 wusang@csc.com.cn

创新业务组

高雪 010-86451347 gaoxue@csc.com.cn

杨曦 -85130968 yangxi@csc.com.cn

李静 010-85130595 lijing@csc.com.cn

黄谦 010-86451493 huangqian@csc.com.cn

王罡 021-68821600-11 wanggangbj@csc.com.cn

诺敏 010-85130616 nuomin@csc.com.cn

上海销售组

李祉瑶 010-85130464 lizhiyao@csc.com.cn

黄方禅 021-68821615 huangfangchan@csc.com.cn

戴悦放 021-68821617 daiyuefang@csc.com.cn

沈晓瑜 shenxiaoyu@csc.com.cn

翁起帆 021-68821600 wengqifan@csc.com.cn

李星星 021-68821600-859 lixingxing@csc.com.cn

范亚楠 021-68821600-857 fanyanan@csc.com.cn

李绮绮 021-68821867 liqiqi@csc.com.cn

薛姣 021-68821600 xuejiao@csc.com.cn

王定润 wangdingrun@csc.com.cn

深广销售组

曹莹 0755-82521369 caoyingzgs@csc.com.cn

张苗苗 020-38381071 zhangmiaomiao@csc.com.cn

XU SHUFENG 0755-23953843 xushufeng@csc.com.cn

程一天 0755-82521369 chengyitian@csc.com.cn

廖成涛 0755-22663051 liaochengtao@csc.com.cn

陈培楷 020-38381989 chenpeikai@csc.com.cn

评级说明

以上证指数或者深证综指的涨跌幅为基准。

买入：未来 6 个月内相对超出市场表现 15％以上；

增持：未来 6 个月内相对超出市场表现 5—15％；

中性：未来 6 个月内相对市场表现在-5—5％之间；

减持：未来 6 个月内相对弱于市场表现 5—15％；

卖出：未来 6 个月内相对弱于市场表现 15％以上。

重要声明

中信建投证券研究发展部

北京

东城区朝内大街 2 号凯恒中心 B 座 12 层（邮编：100010）

电话：(8610)8513-0588

传真：(8610)6560-8446

上海

浦东新区浦东南路 528 号上海证券大厦北塔 22 楼 2201 室（邮编：200120）

电话：(8621)6882-1612

传真：(8621)6882-1622

深圳

福田区益田路 6003 号荣超商务中心 B 座 22 层（邮编：518035）

电话：（0755）8252-1369

传真：（0755）2395-3859