

## 奇安信 (688561.SH)

## 进击的创新网安龙头

2020年09月17日

——公司首次覆盖报告

投资评级: 买入 (首次)

陈宝健 (分析师)

刘逍遥 (分析师)

chenbaojian@kysec.cn

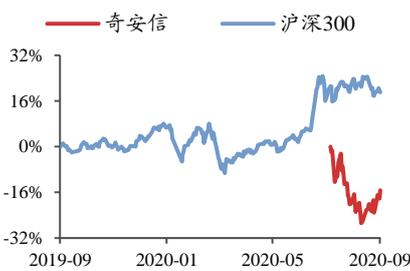
liuxiaoyao@kysec.cn

证书编号: S0790520080001

证书编号: S0790520090001

日期	2020/9/17
当前股价(元)	113.16
一年最高最低(元)	142.66/95.80
总市值(亿元)	769.05
流通市值(亿元)	78.35
总股本(亿股)	6.80
流通股本(亿股)	0.69
近3个月换手率(%)	368.51

### 股价走势图



数据来源: 贝格数据

### ● 高速发展的创新型网络安全领军, 首次覆盖给予“买入”评级

公司是国内创新型网络安全领先厂商, 2017-2019年公司营业收入复合增长率接近96%, 发展势头迅猛。未来随着公司逐渐步入高质量发展阶段, 盈利能力有望提升。我们预测公司2020-2022年归母净利润为-3.28、0.06、4.85亿元, EPS为-0.48、0.01、0.71元/股, 当前股价对应PS为16、11、9倍, 公司PE高于行业可比公司平均水平, PS与行业可比公司平均水平基本持平, 考虑公司为网络安全领军厂商, 正处于业务高速扩张期, 首次覆盖给予“买入”评级。

### ● 高举高打, 高投入铸就强实力

公司保持远高于行业平均水平的投入力度, 打造了强大的产品、服务竞争力及完善的营销体系。技术研发上, 公司重点建设四大研发平台, 打造了面向网安新形势的体系化、协同联动的产品体系。营销体系上, 公司实行“网格化”管理, 将营销体系进一步下沉, 持续向二三线城市及企业级市场发展, 实现商业全覆盖。

### ● 激进式进攻, 意欲引领网安新赛道

新技术、新理念已经成为网络安全市场的重要驱动力, 特别是云安全、威胁情报等新兴安全产品和服务逐步落地, 自适应安全、情境化智能安全等新安全理念接连出现, 为行业发展不断注入创新活力。公司在态势感知、零信任、云安全、代码安全、SD-WAN等新兴领域及“新赛道”重点布局, 并已走在市场前列, 为公司长期发展提供充足的动力。

### ● 紧抓行业需求, 打造精尖安全服务体系

《2017年上半年互联网安全报告》统计显示2020年我国网络安全人才总需求量将达140万人, 人才缺口巨大。公司切中行业需求, 在绵阳设立了人才培养基地&安全运营服务总部, 并建设了覆盖全国的应急响应服务体系, 目前技术支持、安全服务人员已超过2500人, 精尖的安全服务体系也将成为公司未来发展的主要武器。

### ● 风险提示: 商誉减值风险; 持续亏损风险。

### 财务摘要和估值指标

指标	2018A	2019A	2020E	2021E	2022E
营业收入(百万元)	1,817	3,154	4,635	6,582	8,827
YOY(%)	121.2	73.6	46.9	42.0	34.1
归母净利润(百万元)	-872	-495	-328	6	485
YOY(%)	38.4	-43.2	-33.7	-102.0	7443.5
毛利率(%)	55.7	56.7	59.3	60.8	61.9
净利率(%)	-48.0	-15.7	-7.1	0.1	5.5
ROE(%)	-22.3	-11.0	-7.8	0.2	10.3
EPS(摊薄/元)	-1.28	-0.73	-0.48	0.01	0.71
P/E(倍)	-88.2	-155.4	-234.4	11951.5	158.4
P/B(倍)	17.9	15.3	16.4	16.4	14.8

数据来源: 贝格数据、开源证券研究所

## 目 录

1、 高速发展的创新型网络安全领军企业 .....	4
1.1、 业务规模化发展，人效比有望逐渐提升 .....	6
1.1.1、 营业收入高速增长，高投入影响短期利润表现 .....	6
1.1.2、 期间费用率不断降低，经营效益有望逐步提升 .....	7
1.2、 高研发投入铸就核心技术壁垒，产品实力市场领先 .....	7
1.3、 高销售投入搭建完善营销体系，有效促进商机获取 .....	10
2、 激进式进攻，意欲引领网安新赛道 .....	11
2.1、 零信任：网络安全架构的重塑 .....	12
2.2、 态势感知：技术创新力和市场执行力卓越 .....	14
2.3、 EDR：布局早，积累深厚 .....	16
2.4、 SD-WAN：积极抢占快速发展的 SD-WAN 新兴市场 .....	20
2.5、 云安全：云安全管理平台解决方案已在政务云市场占据领先地位 .....	22
3、 产品布局全面，传统赛道亦居领先地位 .....	23
4、 紧抓行业需求，打造精尖安全服务体系 .....	25
5、 盈利预测与投资建议 .....	27
5.1、 关键假设 .....	27
5.2、 盈利预测与投资建议 .....	27
6、 风险提示 .....	27
附： 财务预测摘要 .....	29

## 图表目录

图 1： 公司拥有完善的网络安全产品线和服务体系 .....	5
图 2： 公司控股股东和实际控制人为齐向东先生 .....	5
图 3： 2017-2019 年公司营业收入高速增长 .....	6
图 4： 2017-2019 年公司持续高投入影响利润表现 .....	6
图 5： 公司主要收入来源于网络安全产品、安全服务及配套的硬件收入 .....	6
图 6： 2017-2019 年公司期间费用率变化情况 .....	7
图 7： 公司研发投入力度高于行业平均水平 .....	8
图 8： 奇安信集团位居中国网络安全能力百强——领军者企业矩阵榜首 .....	9
图 9： 公司收入主要来源于“党政军” .....	10
图 10： 公司采取区域与行业相结合的渠道模式 .....	11
图 11： 云安全、零信任网络、SD-WAN 被列入中国 ICT 成熟度曲线中新兴技术范畴 .....	11
图 12： 零信任的关键能力为：以身份为基石、业务安全访问、持续信任评估和总台访问控制 .....	12
图 13： Gartner 预测 2023 年将有 60%的企业从远程访问 VPN 向零信任转型 .....	13
图 14： 奇安信推出零信任解决方案 .....	13
图 15： 奇安信零信任安全解决方案已在某头部客户的大数据中心部署 .....	14
图 16： 中国态势感知市场规模有望在 2021 年达到 54 亿元 .....	14
图 17： 按应用场景来说，态势感知主要分为三类 .....	15
图 18： 奇安信网神态势感知与安全运营平台（NGSOC）引领了国内安全管理产品市场变革 .....	15
图 19： 奇安信 NGSOC 在中国安全管理平台产品市场占有率达到 23.5% .....	16
图 20： 奇安信集团获评中国态势感知解决方案领导者 .....	16

图 21: 公司态势感知平台相关收入均实现高速增长 .....	16
图 22: 中国市场的 EDR 工具提供商可大体分为三类 .....	18
图 23: 奇安信终端一体化家族 .....	19
图 24: 公司曾连续 3 年入选 Gartner 发布的“企业终端防护平台魔力象限” .....	19
图 25: 公司连续 2 年领跑终端安全软件市场 .....	19
图 26: 近三年公司终端安全业务收入年复合增长率超 90% .....	20
图 27: 驱动 SD-WAN 企业部署的四大因素 .....	20
图 28: 2018 年全球 SD-WAN 市场规模为 14 亿美元 .....	21
图 29: 中国 SD-WAN 市场规模有望保持高速增长 .....	21
图 30: 奇安信安全 SD-WAN 实现网络及安全策略一体化编排 .....	22
图 31: 奇安信云安全平台经过国内多家主流云服务厂商官方测试、授权 .....	22
图 32: 2019 年奇安信云安全管理平台凭借 18.1% 的市场份额位列国内第一名 .....	23
图 33: 公司云安全业务收入高速增长 .....	23
图 34: 奇安信是入围全景图细分领域最多的网络安全企业 .....	24
图 35: 奇安信企业级防火墙获全球知名机构 Forrester 推荐 .....	24
图 36: 奇安信入围中国移动 2020-2021 年硬件防火墙集采项目 .....	25
图 37: 公司在中国统一威胁管理硬件市场份额领先 .....	25
图 38: 公司在中国安全内容管理硬件市场份额领先 .....	25
图 39: 2020 年中国网安人才预估缺口 220 万人 .....	26
图 40: 中国网络安全人才需求和供给不匹配 .....	26
图 41: 人才培养绵阳基地作为承载公司安全运营战略主体 .....	26
图 42: 公司技术支持与安服人员数量已超过 2000 人 .....	27
图 43: 规模化、体系化投入攻防演习的攻击和防守 .....	27
表 1: 公司是中国网络安全创新引领者之一 .....	4
表 2: 公司毛利率且与同行业平均水平基本一致 .....	7
表 3: 公司核心技术团队稳定 .....	8
表 4: 公司产品竞争力市场领先 .....	9
表 5: 公司产品及服务具有高复购率 .....	10
表 6: 边界安全与零信任的比较分析 .....	12
表 7: EDR 已经连续 5 年列入 Gartner 公布的十大安全技术/项目 .....	17
表 8: 公司 PE 高于行业可比公司平均水平, PS 与行业可比公司平均水平基本持平 (截止 2020.9.17 收盘) .....	27

## 1、高速发展的创新型网络安全领军企业

脱胎于 360 的企业级网络安全供应商。奇安信成立于 2014 年，原系三六零集团所控制公司。2015 年 12 月，齐向东与周鸿祎及相关方签订了《框架协议》，并于 2016 年 9 月，齐向东及其控制的安源创志完成对奇安信有限增资，齐向东变更为奇安信有限的实际控制人。2019 年 4 月，奇虎科技将所持奇安信有限股权全部转让给明洛投资（中国电子实控企业），公司与 360 集团正式分拆。2020 年 7 月，公司正式登陆科创板。自成立以来公司以高投入研发下的技术创新为引领，特别针对云计算、大数据、移动互联网、工业互联网、物联网等新技术运用下产生的新业态、新场景，为政府与企业等机构客户提供全面有效的网络安全解决方案，成为中国网络安全创新引领者之一。

**表1：公司是中国网络安全创新引领者之一**

时间	发展历程
2014 年	● 公司成立
2015 年	● 提出“数据驱动安全”技术思想
2016 年	● 参与国家重大网络安全 10 次 ● 参与国家护网 2016，协助公安部进行攻防实战演习
2017 年	● 参与国家重大网络安全 13 次 ● 参与国家护网 2017，一带一路攻防演习，辽宁、四川、山东省攻防演习 ● 完成 A 轮融资，估值 116 亿元 ● 提出“四四三三三”技术思想
2018 年	● 参与国家重大网络安全 14 次 ● 完成 B 轮融资，估值 206.5 亿元 ● 参与国家护网 2018，国家发改委、财政部、交通部、水利部、工行和中石油攻防演习
2019 年	● 参与国家重大网络安全 16 次 ● 参与国家护网 2019，财政部、水利部、证监会、国家能源集团、工行、北京市网安总队及海南省攻防演习 ● 提出“内生安全”技术思想 ● 正式成为网络安全“国家队”
2020 年	● 正式登陆科创板

资料来源：公司官网、开源证券研究所

**公司拥有颇为完善的网络安全产品线和服务体系。**公司成立以后，通过对网神和网康的收购，奠定在企业级网络安全市场的发展基础，之后通过不断加大投入、完善布局，目前已经形成较为全面的产品和服务体系。公司产品体系覆盖政企行业网络安全的细分领域，包括三大类别：基础架构安全产品、新一代 IT 基础设施防护产品以及大数据智能安全检测与管控产品。

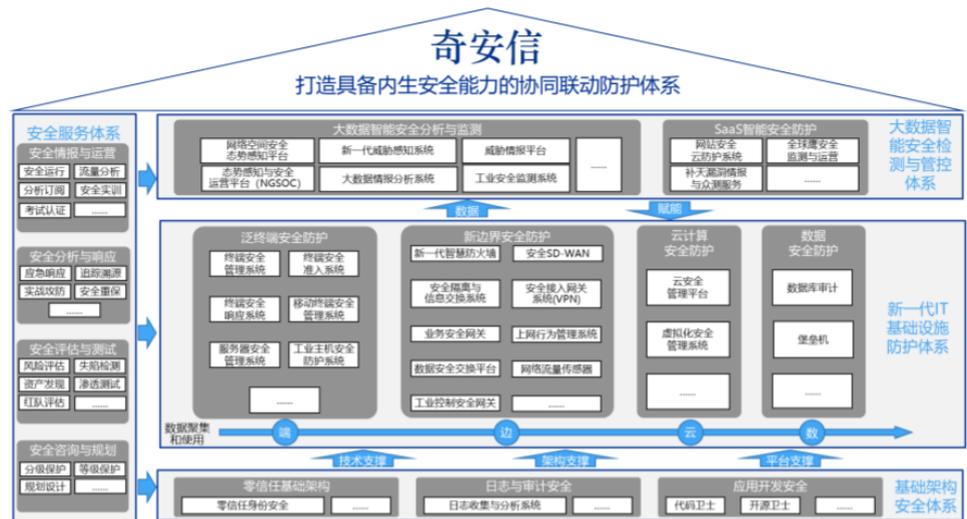
**第一类是基础架构安全类产品**，包括以身份为中心进行动态访问控制的零信任安全产品、针对行为进行审计的日志与审计安全产品以及围绕应用开发的安全产品。

**第二类是新一代 IT 基础设施防护产品**，包括泛终端安全防护、新边界安全防护、云计算基础设施安全防护、大数据基础设施安全防护等产品。

第三类是大数据智能安全检测与管控产品，包括威胁检测、态势感知、安全管理等产品，充分利用大数据分析人工智能方法，为客户提供检测、感知、分析、响应等能力。

同时，公司具备较完善的安全服务体系，以攻防技术与大数据分析为核心，针对不同客户、不同阶段的安全需求，提供咨询与规划、评估与测试、分析与响应、情报与运营等一系列服务。

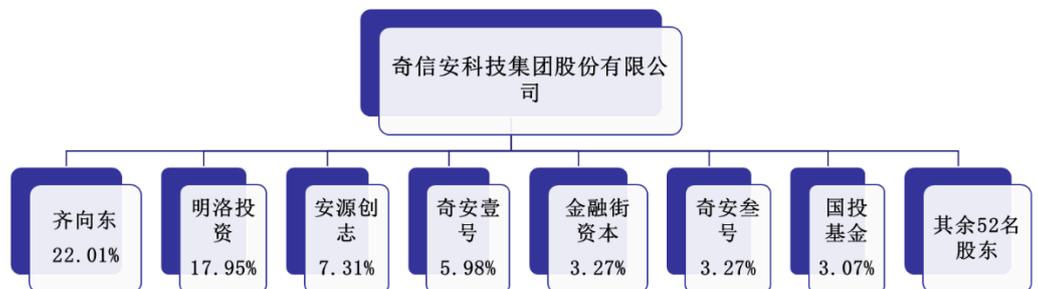
图1: 公司拥有完善的网络安全产品线和服务体系



资料来源：公司招股说明书

中国电子集团入股，成为网络安全“国家队”。公司控股股东和实际控制人为齐向东先生，齐向东先生直接持有公司 22.01%的股份，通过其控制的安源创志、奇安叁号间接控制公司 10.58%的股份，合计控制公司 32.59%的股份。2019 年 5 月，中电金投控股有限公司旗下明洛投资以 37.31 亿元入股奇安信，成为公司的第二大股东，目前持有公司 17.95%股权，中国电子的入股进一步拓展了公司在技术创新、资源整合、重大项目建设等方面的运筹能力。

图2: 公司控股股东和实际控制人为齐向东先生



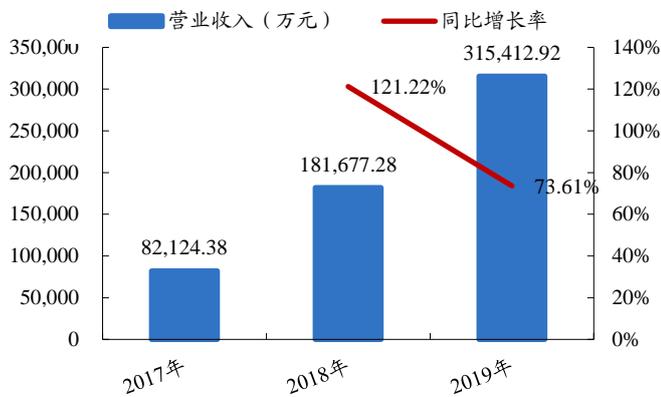
资料来源：公司招股说明书、开源证券研究所

## 1.1、业务规模化发展，人效比有望逐渐提升

### 1.1.1、营业收入高速增长，高投入影响短期利润表现

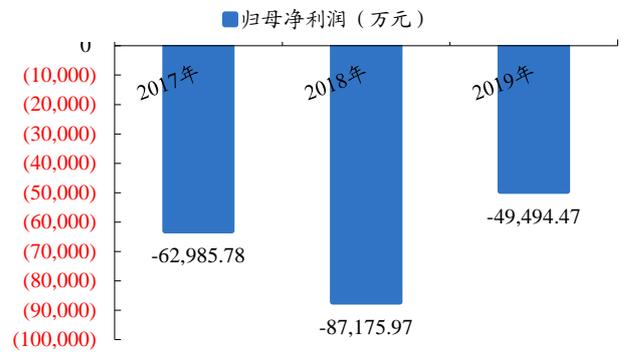
近三年公司营业收入 CAGR 为 96%。2017 年至 2019 年，公司营业收入分别为 8.21 亿、18.17 亿、31.54 亿，近 3 年年均复合增长率为 95.98%，远高于同行业公司平均增速。我们认为公司业务的高速增长主要得益于：1) 高研发投入下公司打造了较强的产品及服务竞争力；2) 完善的销售体系助力公司快速进行客户拓展。同期，归母净利润分别为-6.3 亿元、-8.72 亿元和-4.95 亿元，持续亏损的主要原因是公司选择了高研发投入且人员快速扩张的发展模式，为建设四大研发平台、布局“新赛道”产品、提升攻防竞争力、建立全国应急响应中心而进行了大量投入，各项费用支出远高于行业平均水平。

图3：2017-2019 年公司营业收入高速增长



数据来源：Wind、开源证券研究所

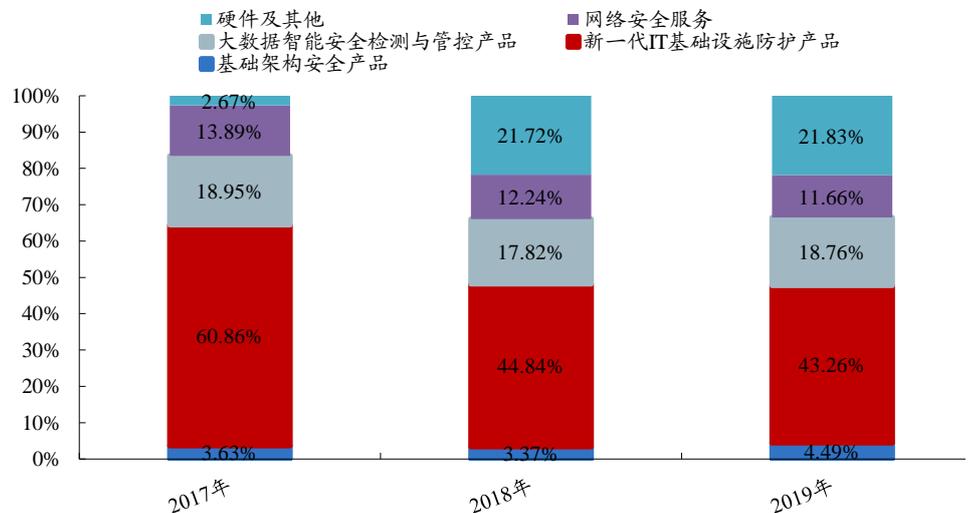
图4：2017-2019 年公司持续高投入影响利润表现



数据来源：Wind、开源证券研究所

公司主要收入来源于网络安全产品、安全服务及配套的硬件收入。具体来看，2019 年网络安全产品占比最高，其中基础架构安全产品收入占比 43.26%，大数据智能安全检测与管控产品收入占比为 18.76%，基础架构安全产品为 4.49%。此外，安全服务收入占比为 11.66%，硬件及其他收入占比为 21.83%。

图5：公司主要收入来源于网络安全产品、安全服务及配套的硬件收入



数据来源：公司招股说明书、开源证券研究所

### 1.1.2、期间费用率不断降低，经营效益有望逐步提升

**安全产品及服务业务毛利率保持较高水平。**2017-2019年，公司综合毛利率分别为74.91%、55.68%及56.72%，2018年及2019年毛利率较2017年下滑幅度较大的主要原因为毛利率较低的硬件及其他业务收入占比提升较大。在剔除硬件及其他业务收入后，2017-2019年公司的网络安全产品及服务综合毛利率水平分别为76.30%、70.07%和71.63%，核心业务毛利率水平整体保持较高水平，且与同行业平均水平基本一致。

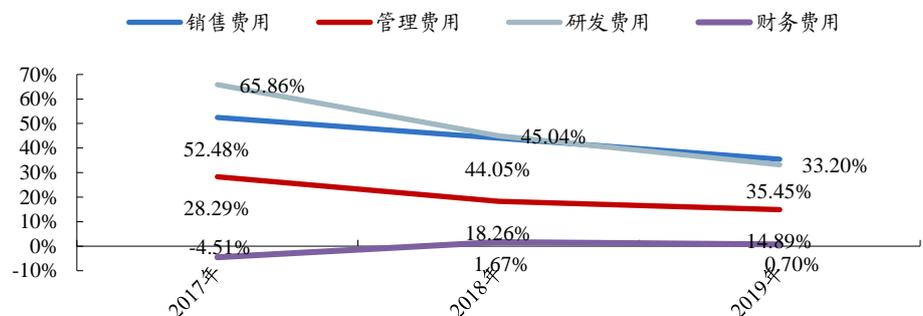
**表2：公司毛利率且与同行业平均水平基本一致**

年份	项目	启明星辰	绿盟科技	安恒信息	南洋股份	平均值	奇安信
2019年	网络安全产品	64.96%	72.15%	77.59%	61.32%	<b>69.01%</b>	<b>73.1%</b>
	网络安全服务	67.87%	74.39%	54.26%	65.3%	<b>65.46%</b>	<b>63.24%</b>
	硬件及其他	-	2.85%	0.71%	-	<b>1.78%</b>	<b>3.18%</b>
2018年	网络安全产品	76.63%	78.06%	75.15%	65.45%	<b>73.82%</b>	<b>72.48%</b>
	网络安全服务	54.93%	83.36%	65.69%	64.37%	<b>67.09%</b>	<b>57.06%</b>
	硬件及其他	14.91%	19.26%	7.51%	-	<b>13.89%</b>	<b>1.36%</b>
2017年	网络安全产品	76.89%	76.25%	72.14%	78.09%	<b>75.84%</b>	<b>77.61%</b>
	网络安全服务	45.23%	75.98%	61.5%	82.36%	<b>66.27%</b>	<b>68.39%</b>
	硬件及其他	8.98%	9.53%	4.04%	-	<b>7.52%</b>	<b>4.92%</b>

数据来源：公司招股说明书、Wind、开源证券研究所

**投入规模持续扩大，期间费用率逐渐降低。**为巩固竞争优势与行业地位，公司不断增加研发和销售投入，期间费用持续增长。但公司期间费用占应收的比例不断下降。根据公司招股说明书，公司逐渐建立了技术壁垒、品牌优势，同时研发及销售费用投入收入占比逐渐降低。公司积累的技术优势、品牌优势将通过规模效应显现，目前已经呈现“提效降费”的盈利趋势，未来实现盈利高速增长可期。公司招股说明书披露，根据企业管理层的测算，预计研发费用占比将降低至26%-28%区间，销售费用占比将降低至30%-32%区间，以60%-62%的毛利率为经营目标的情况下，预计公司在收入达到44-46亿元时可实现盈亏平衡，之后将实现盈利。

**图6：2017-2019年公司期间费用率变化情况**

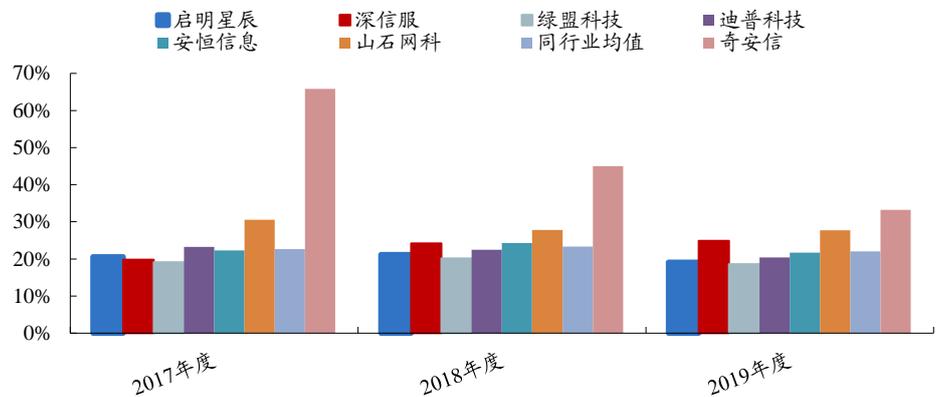


数据来源：公司招股说明书、开源证券研究所

## 1.2、高研发投入铸就核心技术壁垒，产品实力市场领先

公司自成立以来一直高度重视研发，具备行业内领先的技术研发能力，研发人员规模及研发投入规模不断扩大。2017-2019年，公司研发人员从1541人增长至2591人，年均复合增长率为29.67%；研发投入分别为54,083.45万元、81,834.51万元和104,710.40万元，占营业收入的比例分别为65.86%、45.04%和33.20%，高于行业平均水平。

图7：公司研发投入力度高于行业平均水平



数据来源：公司招股说明书、开源证券研究所

**核心技术团队稳定。**公司核心技术团队大多曾任职于三六零集团、绿盟、网康等国内领先的网安企业。其中，公司总裁吴云坤先生曾任中联绿盟信息技术（北京）有限公司副总裁，三六零集团企业安全总裁。目前担任中国信息协会信息化促进工作委员会副主任、中国指挥与控制学会网络空间安全专业委员会副主任委员、中国人民公安大学网络空间安全与法治协同创新中心专家组专家、广州中科院软件应用技术研究所电子数据取证实验室专家委员会专家、工业互联网战略咨询专家委员会委员，被《中国信息安全》杂志社评为2018年度中国信息安全产业“领军人物”。

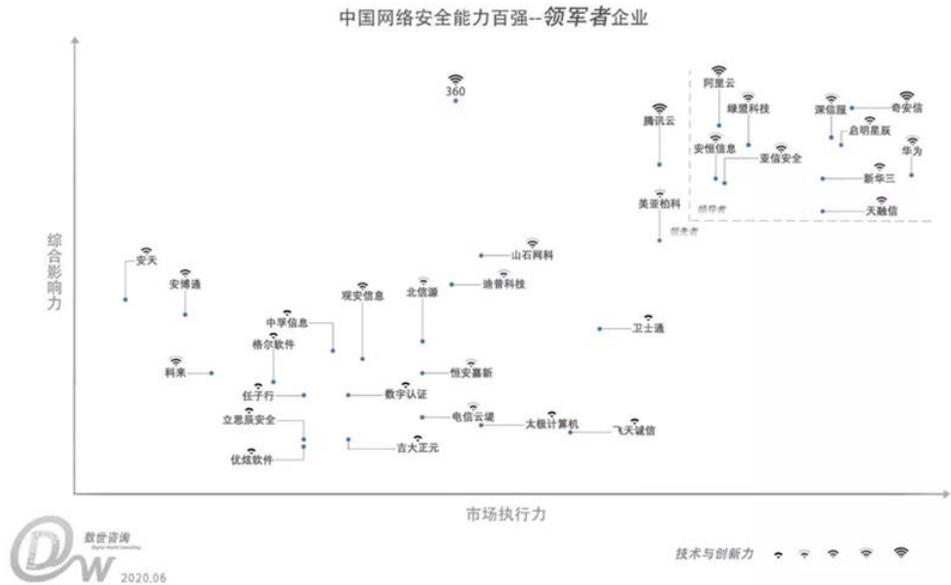
表3：公司核心技术团队稳定

姓名	职位	履历
吴云坤	总裁	曾任中联绿盟信息技术（北京）有限公司副总裁，三六零集团企业安全总裁
徐贵斌	副总裁、华南基地负责人	曾任三六零集团技术总监
马江波	大数据及安全运营业务总经理	曾任北京神州绿盟科技有限公司技术总监，云脑安御首席技术官
刘浩	云安全业务线总经理	曾任三六零集团高级技术经理、运维开发部负责人、云事业部技术总监
左文建	副总裁、总工办主任	曾任三六零集团技术总监、北京达客优家信息技术有限公司首席技术官、网神股份部门负责人、聪投（北京）信息技术有限公司首席技术官
刘岩	智能安全网络事业部副总经理	曾任北京网康科技高级软件工程师、高级工程师、研发总监
吴勇义	大数据与态势感知业务线技术总监	曾任观潮会议技术总监
顾永翔	终端安全业务线副总经理	曾任北京铠信神州科技有限责任公司总经理
吉艳敏	终端安全业务线技术总监	曾任三六零集团高级软件工程师

资料来源：公司招股说明书、开源证券研究所

公司的高研发投入有效的转化为公司强大的技术壁垒，并已逐步转化为产品优势。根据国内数字产业第三方调研与咨询机构数世咨询发布《中国网络安全能力 100 强》，奇安信集团位居中国网络安全能力百强——领军者企业矩阵榜首。

图8: 奇安信集团位居中国网络安全能力百强——领军者企业矩阵榜首



资料来源: 数世咨询

公司不仅在终端安全、UTM 等传统安全领域走在市场前列，在云安全、态势感知等新兴领域也处于领先地位。根据赛迪咨询、IDC 等第三方机构的报告，公司在新一代 IT 基础设施防护产品体系中的终端安全领域、大数据智能安全检测与管控产品体系中的安全管理平台和云安全领域、安全服务市场份额第一，公司终端安全技术、第三代安全引擎技术、大数据安全分析技术、漏洞挖掘技术、软件定义安全技术、威胁情报技术等处于行业领先地位。

表4: 公司产品竞争力市场领先

项目	2018 年排名	2017 年排名	数据来源
终端安全	1	2	赛迪咨询
安全管理平台	1	2	赛迪咨询
安全服务	1	2	赛迪咨询
云安全	1		赛迪咨询
Web 安全	2	2	赛迪咨询
UTM	2	2	赛迪咨询
终端安全软件	1	2	IDC
安全内容管理硬件	2	2	IDC

资料来源: 公司招股说明书、赛迪咨询、IDC、开源证券研究所

高复购率进一步印证了公司产品线丰富、产品及服务满意度高。2017-2019 年，公司收入中由老客户采购带来的部分占比分别为 28.53%、61.27%和 58.49%，2018、2019 年老客户采购对收入增长的贡献较 2017 年有较大提升。公司历年的老客户，会在新的采购周期中带来复购，主要原因为: (1) 新客户在首次选择网络安全产品或服务时，通常先购买一部分产品，使用后如满足相关需求或对产品和服务相对满意，则会在后续采购时从相应供应商加购相关产品; (2) 公司的产品线较丰富，新客户购买

其中某个/某些产品后，后续可能增加购买其他产品线或产品，故老客户复购时的单价普遍高于新客户。

**表5: 公司产品及服务具有高复购率**

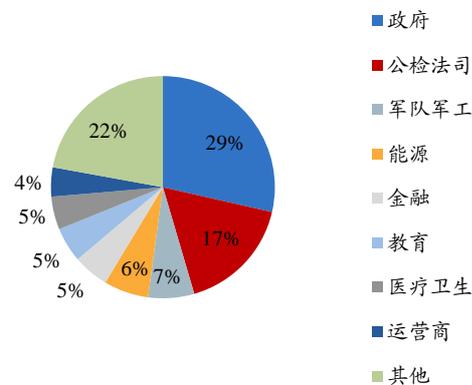
	2017年		2018年		2019年		客单价 (万元)
	收入 (万元)	数量	收入 (万元)	数量	收入 (万元)	数量	
老客户	184,199.48	5,127	110,225.13	3,278	22,955.48	1,261	18.20
新客户	130,734.00	11,746	69,267.97	7,449	57,506.81	7,029	8.18
合计	314,933.48	16,873	179,493.10	10,727	80,462.29	8,290	9.71

数据来源：公司招股说明书、开源证券研究所

### 1.3、高销售投入搭建完善营销体系，有效促进商机获取

“网格化”管理，推动营销体系下沉。公司一直以网络安全的急迫性为前提，以优先满足“党政军”（政府、公检法司、军队军工）需求为核心保障，以涉及民生的重点基础行业（能源、金融、医疗卫生、运营商等）为重点扩展，不断拓展提升商业市场份额，采取的具体措施是“网格化”管理，将营销体系进一步下沉，持续向二三线城市及企业级市场发展，实现商业全覆盖。

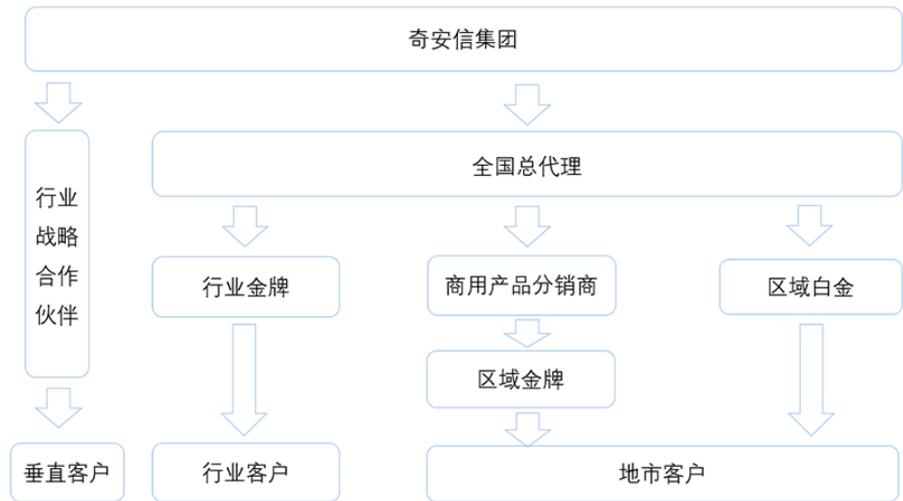
**图9: 公司收入主要来源于“党政军”**



数据来源：公司招股说明书、开源证券研究所

**直销+分销的模式力争最大的客户覆盖面。**对于大中型政企客户，公司一般采用直销的方式，安排专门的销售及业务团队为其进行服务，以满足其独特的安全需求；对于其他客户，公司的产品具有广阔的适用性，则一般采取渠道销售的方式，最大限度地覆盖更多客户的需求，提高公司的市场占有率。在渠道体系建设方面，公司采取了区域与行业相结合的渠道模式，其中区域经销体系主要基于以上海佳电为全国总经销商的多层次区域经销体系，各层级经销商在市场拓展、渠道建设等方面各有分工；行业渠道商主要覆盖政府、公检法司等重点行业客户，包括经销和项目合作两种模式。

图10: 公司采取区域与行业相结合的渠道模式



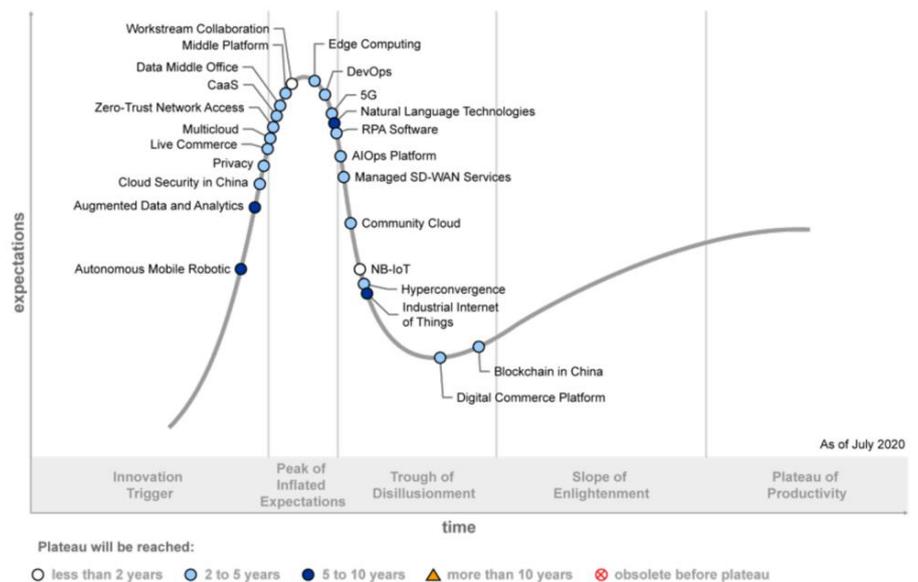
资料来源: 公司官网、开源证券研究所

## 2、激进式进攻，意欲引领网安新赛道

新技术、新理念已经成为网络安全市场的重要驱动力。云安全、威胁情报等新兴安全产品和服务逐步落地，自适应安全、情境化智能安全等新的安全防护理念接连出现，为网络安全技术发展不断注入创新活力。根据 Gartner 最新发布的《2020 年中国 ICT 技术成熟度曲线》，云安全、零信任网络、SD-WAN 都被列入新兴技术范畴，安恒信息、绿盟、奇安信、深信服等厂商凭借领先的技术实力入选报告。

图11: 云安全、零信任网络、SD-WAN 被列入中国 ICT 成熟度曲线中新兴技术范畴

Hype Cycle for ICT in China, 2020



Source: Gartner  
ID: 448134

资料来源: Gartner 《2020 年中国 ICT 技术成熟度曲线》

公司在终端安全、大数据态势感知、云安全、代码安全、SD-WAN、工业安全、

身份安全、物联网安全等新兴领域及“新赛道”重点布局，与当今信息技术发展中重点的发展领域相互匹配。

## 2.1、零信任：网络安全架构的重塑

零信任架构是一种网络/数据安全的端到端的方法，提供一系列概念、理念、组件及其交互关系，以便消除针对信息系统和服务进行精准访问判定所存在的不确定性。零信任的技术本质是以身份为基石的动态可信访问控制，聚焦身份、信任、业务访问和动态访问控制等维度的安全能力，基于业务场景的人、流程、环境、访问上下文等多维的因素，对信任进行持续评估，并通过信任等级对权限进行动态调整，形成具备较强风险应对能力的动态自适应的安全闭环体系。

图12：零信任的关键能力为：以身份为基石、业务安全访问、持续信任评估和总台访问控制



资料来源：奇安信集团

零信任的理念已经从边界模型的“信任但验证”转换到“从不信任始终验证”的模式。正如 Evan Gilman《Zero Trust Networks》一书所述，零信任网络建立在五个假设前提之下：1) 应该始终假设网络充满威胁；2) 外部和内部威胁每时每刻都充斥着网络；3) 不能仅仅依靠网络位置来确认信任关系；4) 所有设备、用户、网络流量都应该被认证和授权；5) 访问控制策略应该动态地基于尽量多的数据源进行计算和评估。

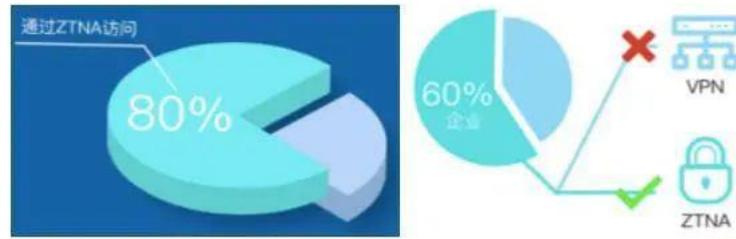
表6：边界安全与零信任的比较分析

边界安全	零信任
以“网络安全”为中心	以“应用和数据安全”为中心
外访“坏人”	外访“坏人”、内控“好人”
以“信任”为基础的访问控制	以默认“零信任”为基础的访问控制
静态的访问控制策略	基于信任的动态访问控制策略
资源对外可见不可用	资源对外不可用不可见，可用不可见

资料来源：绿盟科技、开源证券研究所

随着云计算、大数据等新兴技术的广泛采用，零信任不断演进，以身份为基石的架构体系得到业内主流认可。根据 Gartner 预测，2022 年将有 80% 面向生态合作伙伴的新数字业务应用采用零信任网络访问。2023 年将有 60% 的企业从远程访问 VPN 向零信任网络架构转型。

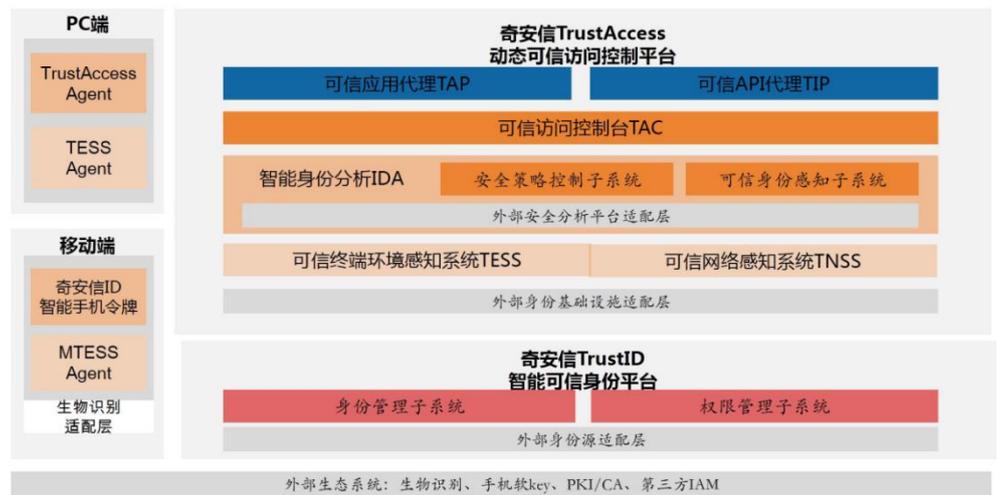
图13: Gartner 预测 2023 年将有 60%的企业从远程访问 VPN 向零信任转型



资料来源: Gartner

奇安信身份安全实验室是公司旗下专注研究“零信任安全架构”的专业实验室，团队以“零信任安全，新身份边界”为核心理念，推出以“以身份为基石、业务安全访问、持续信任评估和总台访问控制”为四大关键能力的解决方案。奇安信零信任解决方案主要包括：奇安信 TrustAccess 动态可信访问控制平台、奇安信 TrustID 智能可信身份平台、奇安信 ID 智能手机令牌、及各种终端 Agent 组成。

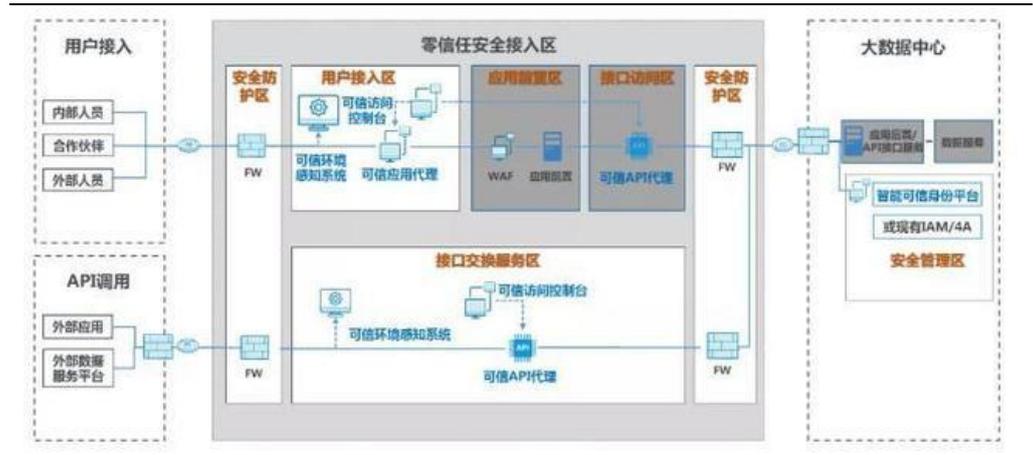
图14: 奇安信推出零信任解决方案



资料来源: 奇安信集团

奇安信零信任架构安全解决方案已在部委级客户、能源企业、金融行业等进行正式的部署建设或 POC 试点。以零信任安全架构方案在大数据中心应用为例，奇安信零信任安全解决方案在某头部客户的大数据中心已大规模持续稳定运行超过半年，通过零信任安全接入区，覆盖应用达到 60 多个，用户终端超过 1 万，每天的应用访问次数超过 200 万次，数据流量超过 600G，有效保证了相关大型组织对大数据中心的安全。

图15: 奇安信零信任安全解决方案已在某头部客户的大数据中心部署

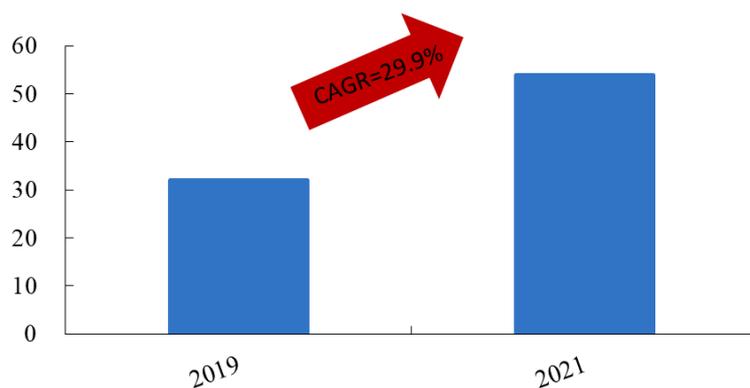


资料来源: 奇安信集团

## 2.2、态势感知: 技术创新力和市场执行力卓越

态势感知是仍处于快速增长期的网安细分市场。态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力,是以安全大数据为基础,从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式,最终是为了决策与行动,是安全能力的落地。在2016年419网络安全和信息化工作座谈会上,习近平总书记提出“要树立正确的网络安全观,加快构建关键信息基础设施安全保障体系,全天候全方位感知网络安全态势,增强网络安全防御能力和威慑能力。”态势感知首次被提升到了国家高度,并迅速成为网络安全领域的热点。根据数世咨询调研统计,2019年国内态势感知市场规模约在32亿元左右,预计2021年将达到54亿元左右。

图16: 中国态势感知市场规模有望在2021年达到54亿元



数据来源: 数世咨询、开源证券

数世咨询从应用场景(使用对象)的角度将态势感知分为三大类: 1) 政府监管类, 政府监管部门对监管范围内的全网网络安全状态进行监督管理, 包括对攻击、威胁与风险态势的掌握, 以及定位安全事件和对责任方进行通告。2) 行业监管类, 主要用于对带有行业性质的所属下级单位的监督管理。掌握本行业的安全态势, 并对本行业下属机构的安全工作进行指导性的组织与协调。3) 机构运营类, 运营类态势感知主要用于机构和企业自身的网络安全管理与保障工作。

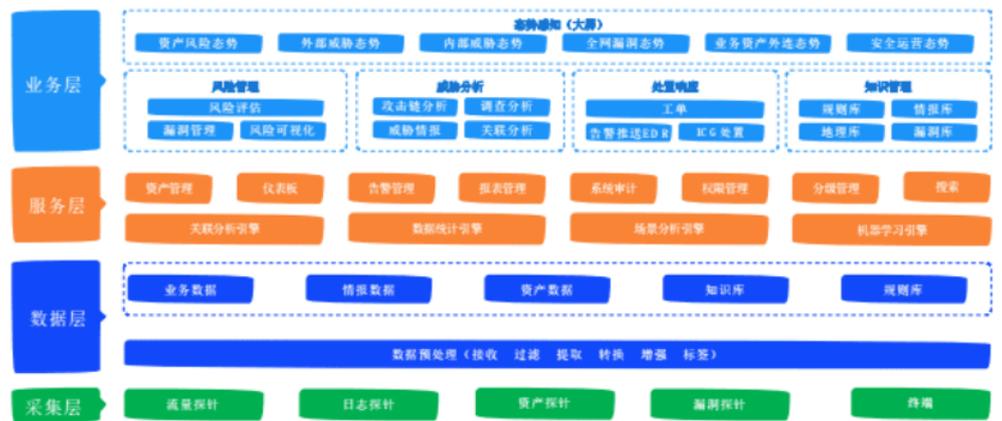
图17: 按应用场景来说, 态势感知主要分为三类



资料来源: 数世咨询、开源证券

奇安信网神态势感知与安全运营平台 (NGSOC) 引领了国内安全管理产品市场变革, 也获得了众多客户的认可。NGSOC 以大数据平台为基础, 通过收集多元、异构的海量日志, 利用关联分析、机器学习、威胁情报等技术, 帮助政企客户持续监测网络安全态势, 实现从“被动防御”向“积极防御”的进阶, 为安全管理者提供风险评估和应急响应的决策支撑, 为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具, 目前已在 400+大型政企单位落地实践。

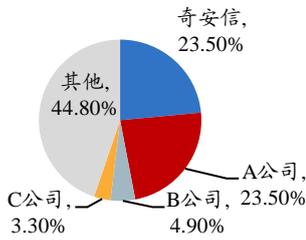
图18: 奇安信网神态势感知与安全运营平台 (NGSOC) 引领了国内安全管理产品市场变革



资料来源: 公司官网

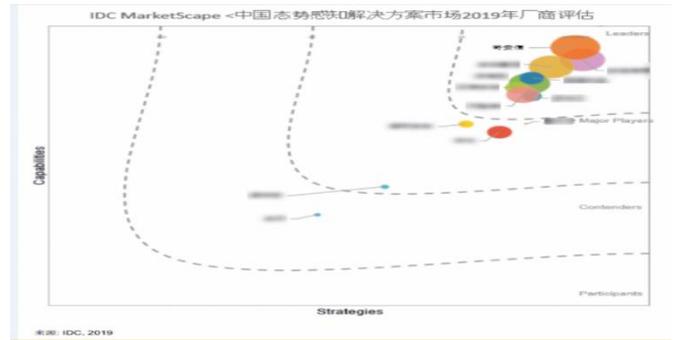
赛迪顾问发布的《2018-2019 年中国网络信息安全市场研究年度报告》显示, 奇安信 NGSOC 在中国安全管理平台产品市场占有率达到 23.5%, 排名第一。IDC 发布的《中国态势感知解决方案市场 2019 年厂商评估》显示, 奇安信集团获评中国态势感知解决方案领导者。数世咨询发布的态势感知能力点阵图显示, 奇安信态势感知在技术创新力和市场执行力均处于领导者地位。

图19: 奇安信 NGSOC 在中国安全管理平台产品市场占有率达到 23.5%



数据来源: 赛迪顾问《2018-2019 年中国网络信息安全市场研究年度报告》、开源证券研究所

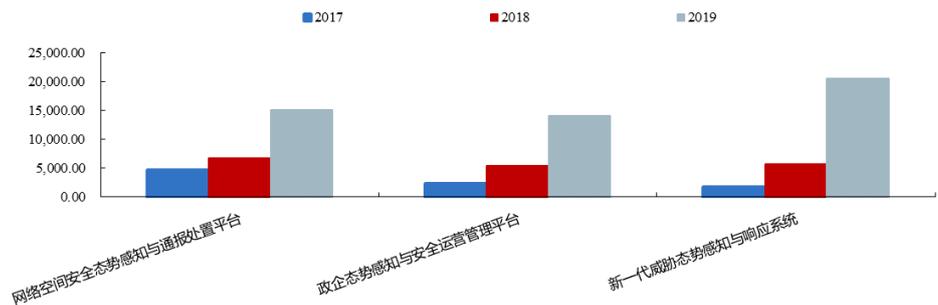
图20: 奇安信集团获评中国态势感知解决方案领导者



资料来源: IDC

公司态势感知平台相关收入均实现高速增长。2017-2019 年,“网络空间安全态势感知与通报处置平台”、“政企态势感知与安全运营管理平台 (NGSOC)”及“新一代威胁态势感知与响应系统”收入的年复合增长率分别为 80.3%、143.9%和 239.1%。

图21: 公司态势感知平台相关收入均实现高速增长



数据来源: 公司招股说明书、开源证券研究所

### 2.3、EDR: 布局早, 积累深厚

EDR (端点检测和响应) 是一种主动式端点安全解决方案。Gartner 将“端点检测和响应解决方案市场”定义为“记录和存储端点系统级别的行为, 使用各种数据分析技术来检测可疑的系统行为, 提供上下文信息, 阻止恶意活动并提供补救建议以恢复受影响的系统的解决方案”。相比于传统端点安全防护采用预设安全策略的静态防御技术, EDR 加强了威胁检测和响应取证能力, 能够快速检测、识别、监控和处理端点事件, 从而在威胁尚未造成危害前进行检测和阻止, 帮助受保护网络免受零日威胁和各种新出现的威胁。

EDR 作为终端安全领域的热门技术, 已经连续 5 年列入 Gartner 公布的十大安全技术或项目。IDC 认为, 传统终端安全防护平台 (EPP) 产品虽然保持着平稳的增长, 但相对于全球整体网络安全市场的发展态势, 增速已经明显偏低; 与此同时, 终端安全检测与响应 (EDR) 工具的作用和重要性在全球已经得到了安全企业及最终用户的广泛认可, 并将成为未来几年终端安全市场持续增长的重要推动力之一。

**表7: EDR 已经连续 5 年列入 Gartner 公布的十大安全技术/项目**

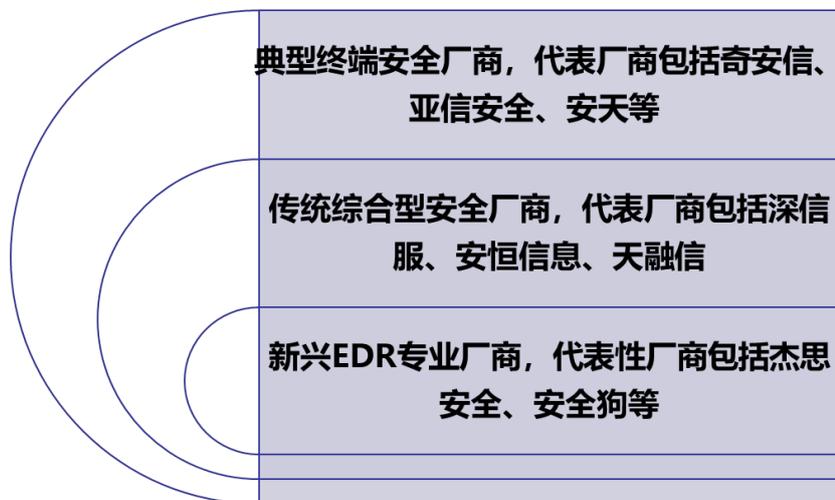
	2014 年	2016 年	2017 年	2018 年	2019 年
身份和访问管理 IAM	自适应访问控制				
云安全	软件定义的安全 (SDS)				
	云访问安全代理 (CASB)	云访问安全代理 (CASB)	云访问安全代理 (CASB)	云访问安全代理 (CASB)	云访问安全代理 (CASB)
	微隔离		微隔离		
	云工作负载保护平台 (CWPP)			云安全配置管理 (CPSM)	云安全配置管理 (CPSM)
端点安全	端点检测与响应 (EDR)	端点检测与响应 (EDR)	端点检测与响应 (EDR)	端点检测与响应 (EDR)	端点检测与响应 (EDR)
	基于非签名方法的端点防御技术				
					服务器工作负载的应用控制
网络安全	遏制与隔离讲作为基础的安全策略		远程浏览器	远程浏览器	
			欺骗技术	欺骗技术	检测与响应的欺骗技术
	网络流量分析 (NTA)				
	及其可识别的威胁情报 (包括信管服务)				
	沙箱普遍化				
应用安全			用户和实体行为分析 (UEBA)	检测与响应之 UEBA	
	交互式应用安全测试	DevOps 的安全测试技术	面向 DevOps 的软件安全扫描与软件成分分析	字段安全扫描: 面向 DevOps 的软件成分分析	
				容器安全	容器安全
数据安全					暗数据发现
IoT	针对物联网安全的网关、代	普适信任服务			

	2014年	2016年	2017年	2018年	2019年
	理和防火墙				
	大数据安全分 析技术是下一 代安全平台的 核心	情报驱动的安 全运营中心及 编排解决方案 技术	可管理检测与 响应 NDR	检测与响应之 NDR	
安全运营				符合 CARTA 的弱点管理	符合 CARTA 的弱点管理
					安全事件响应
					安全评级服务

资料来源：安全牛、Gartner、开源证券研究所

中国市场的 EDR 工具提供商可大体分为三类：一是典型终端安全厂商，利用终端安全领域的长期技术积累并配合自有终端杀毒引擎，形成 EPP+EDR 的综合终端防护方案，代表性厂商包括奇安信、亚信安全、安天等；二是传统综合型安全厂商，利用全面的技术能力和市场优势打造专业的 EDR 工具，并通过技术合作、生态建设等多种方式优化完善终端安全方案，代表性厂商包括深信服、安恒信息、天融信等；三是新兴 EDR 专业厂商，凭借自身独特的技术能力和产品创新优势，正在成为终端安全检测与响应市场的重要玩家，代表性厂商包括杰思安全、安全狗等。

图22：中国市场的 EDR 工具提供商可大体分为三类



资料来源：公司招股说明书、开源证券研究所

奇安信天擎终端安全产品一开始就致力于“规划-实施-合规-攻防”的全生命周期能力，提供一体化的终端保护解决方案，在传统防病毒能力上具有领先的能力和积累，EDR 布局早，跟进速度更快，在行业内处于领先水平。公司终端安全产品对 360 集团不存在过分技术依赖，已推出自主的终端安全产品。公司对三六零集团技术的使用主要集中于面向政企客户与面向个人用户端技术有一定重合度的终端安全领域，具体产品为一体化终端管理（天擎）产品。2019 年 7 月，公司推出了自主研发的奇安信终端安全产品（新版天擎）。就天擎的前述九大功能模块之与面向个人用户的终端安全产品重叠的“终端安全防护”功能模块中，通过自研技术对三六零集团的技术进行了剔除，发行人均具有相关知识产权，不存在侵权 360 的情况。2020 年 4

月，新版奇安信终端安全产品通过了国际权威反病毒实验室 Virus Bulletin1 组织的 VB100 测评。该产品在零误报的前提下，以 100% 多样化样本检出率检出了全部病毒。自 2019 年 7 月新版奇安信终端安全产品发布以来，已签署超过 8,000 张订单，覆盖超过 380 万个政企终端。

图23: 奇安信终端一体化家族



资料来源: 公司官网

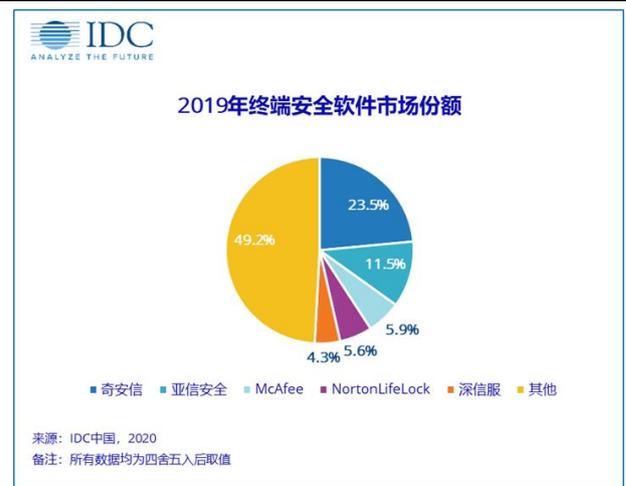
公司曾连续 3 年入选 Gartner 发布的“企业终端防护平台魔力象限”。公司天擎 EDR 也是首家通过赛可达威胁检测能力测试的国内 EDR 产品。根据 IDC 发布的《2019 年下半年中国 IT 安全软件市场跟踪报告》，在终端安全领域，公司以 23.5% 的市场份额，领跑终端安全软件市场，相比 2018 年 22.9% 的市场份额增长了 0.6 个百分点。

图24: 公司曾连续 3 年入选 Gartner 发布的“企业终端防护平台魔力象限”

图25: 公司连续 2 年领跑终端安全软件市场



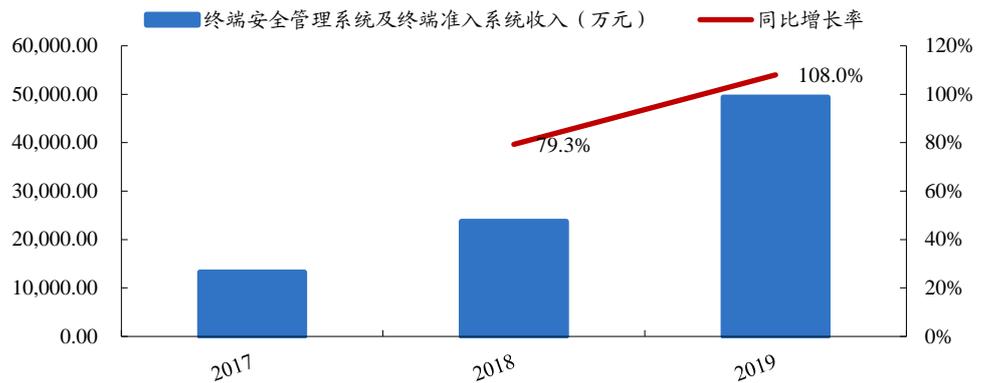
资料来源: Gartner



资料来源: IDC

近三年公司终端安全业务收入年复合增长率超 90%。2017-2019 年，公司终端安全管理系统及终端准入系统的营业收入分别为 13,245.48 万元、23,750.85 万元和 49,402.68 万元，年均复合增长率为 93.13%。

图26: 近三年公司终端安全业务收入年复合增长率超 90%



数据来源: 公司招股说明书、开源证券研究所

## 2.4、SD-WAN: 积极抢占快速发展的 SD-WAN 新兴市场

SD-WAN 能够大大提高网络灵活性和组网效率。SD-WAN 以网络即服务(NaaS) 和安全即服务(SaaS)的方式,为分支机构与总部互联、多个数据中心互联、多个混合云互联等场景的用户提供广域安全组网方案。安全 SD-WAN 由安全网络路由网关系统和安全网络管控平台,安全网络路由网关系统为企业总部、数据中心或者分支机构之间的互联提供组网和安全防护功能,安全网络管控平台对安全网络路由网关的网关设备、网络连接、安全功能以及接入的终端和用户进行集中化、可视化的统一控制和管理。主要应用于多分支企业快速组网、企业网络与云数据中心互联、物联网数据回传。

图27: 驱动 SD-WAN 企业部署的四大因素



资料来源: IDC Survey、飞鱼

SD-WAN 的整体成长性取决于需求侧的强劲驱动,例如对降低 MPLS 成本、简化 VPN、降低远程协作成本等真实需求。而伴随着企业将越来越多的应用部署在云端,并且在 IT 基础架构上采用混合云的技术架构,企业的数字化转型进程、SaaS 应用的推广也将带动 SD-WAN 市场的快速增长。据 IDC 预测,作为企业网络市场的一个重要组成部分,全球 SD-WAN 市场将从 2018 年到 2023 年期间以 30.8% 的复合年增长率增长,届时规模将达到 52.5 亿美元,预计这一数字将在未来几年稳步增长。

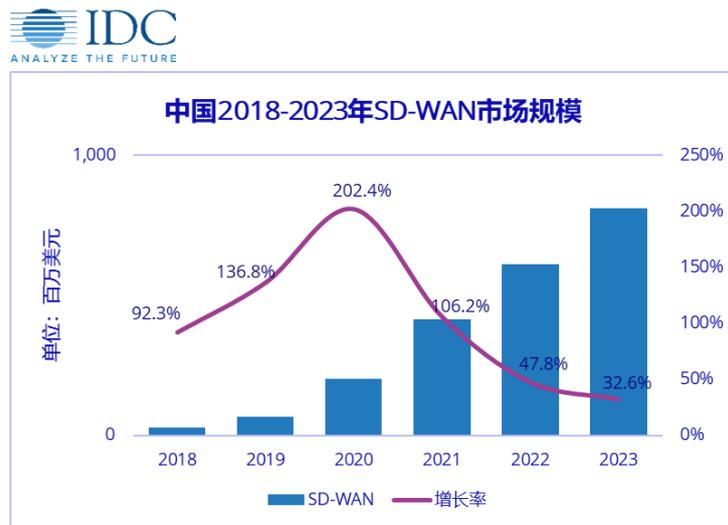
图28: 2018 年全球 SD-WAN 市场规模为 14 亿美元



资料来源: IDC

同时, 根据 IDC 对中国 SD-WAN 市场的初步调研和统计, 中国 SD-WAN 应用始于 2017 年, 在 2018 年快速增长, 2019 年 SD-WAN 市场增速超过 130%, 市场规模接近 7000 万美元, 客户群体遍布金融、零售、制造、互联网、媒体、政府、医疗、能源、电力、教育、交通和服务等多个行业。

图29: 中国 SD-WAN 市场规模有望保持高速增长



来源: IDC中国, 2020

资料来源: IDC 中国

2019 年 3 月, 奇安信正式发布以“智连接, 全守护”为价值主张的安全 SD-WAN 产品。奇安信安全 SD-WAN 解决方案基于安全路由网关内置的用户识别、终端认证功能, 确保接入用户和终端可信, 同时利用深度集成的入侵防御 (IPS)、病毒防护 (AV) 等高级安全特性, 实现了分支与总部间网络的深度安全过滤。2020 年 7 月, 奇安信发布了全新的安全 SD-WAN 2.0, 在零配置上线、自动 VPN 组网、流量调度、安全策略与网络策略统一编排等核心功能的基础上, 新加入了威胁情报能力, 为 SD-WAN 技术应用和市场注入了新的活力。

图30: 奇安信安全 SD-WAN 实现网络及安全策略一体化编排

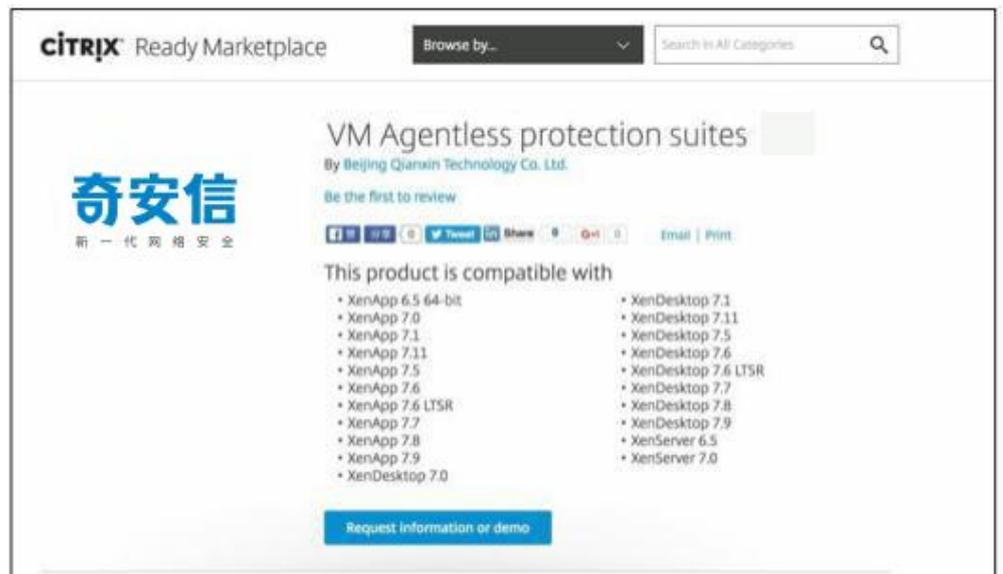


资料来源: 公司官网

### 2.5、云安全: 云安全管理平台解决方案已在政务云市场占据领先地位

最近三年来国内云计算及云安全处于高速增长期, 全国包括政务云、政务大数据、警务云、警务大数据、司法、教育、卫生等行业云及各种央企、大型企业云安全需求激增。公司掌握 VMware、KVM、Xen 三种平台的无代理杀毒和网络防护技术, 2017 年取得“VMware Ready”认证, 在国内厂商中率先推出 VMware 无代理杀毒产品。针对云计算环境生态多样导致的适配性难题, 公司云安全管理产品已适配包括 VMware、华为、浪潮等三十多家厂商的云计算平台, 可以实现对多云场景、容器、虚拟化及裸金属物理服务器的一体化安全防护。

图31: 奇安信云安全平台经过国内多家主流云服务厂商官方测试、授权

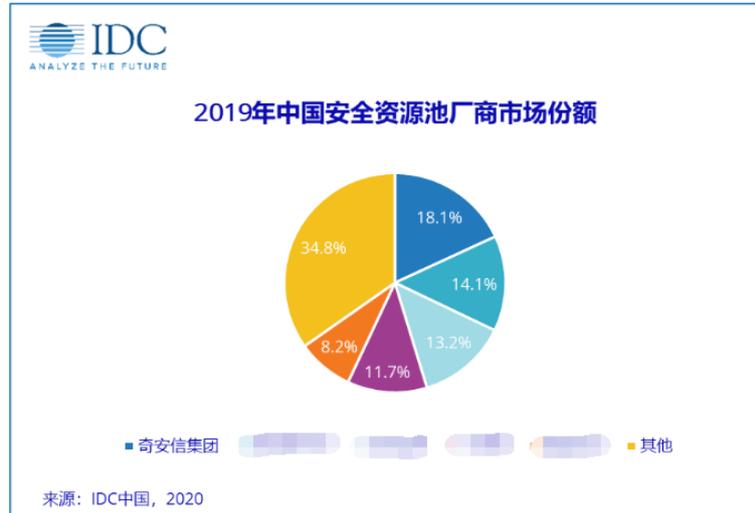


资料来源: 公司官网

奇安信云安全管理平台解决方案已在政务云市场占据领先地位。公司与多家运

营商联合，为吉林省政务云、河南省政务云、湖北省政务云、云上扬州、苏州市政务云、绍兴市政务云、成都市政务云、衡阳市政务云等几十朵政务云提供云安全解决方案，得到客户的广泛认可。根据 IDC 最新发布的报告《中国安全资源池市场份额，2019：新市场、新动能、新发展》，2019 年奇安信云安全管理平台凭借 18.1% 的市场份额，位列国内第一名。

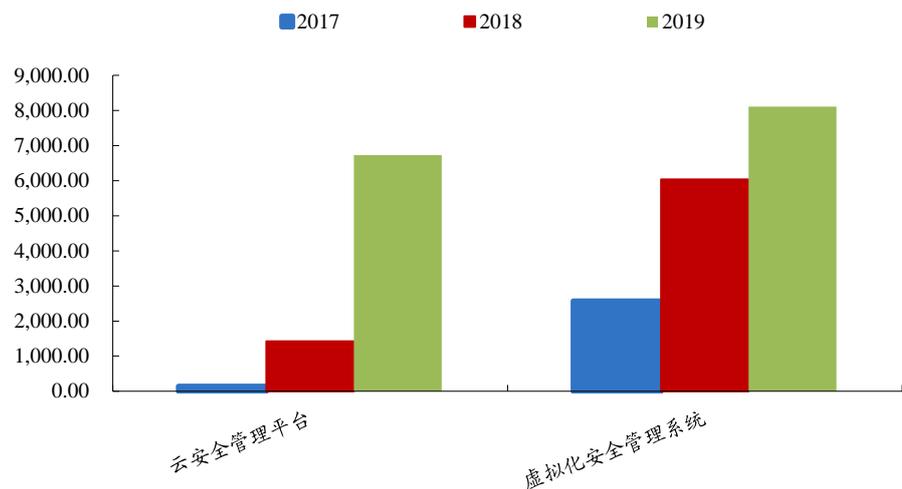
图32: 2019年奇安信云安全管理平台凭借18.1%的市场份额位列国内第一名



资料来源: IDC《中国安全资源池市场份额, 2019: 新市场、新动能、新发展》

公司云安全业务收入高速增长。2017-2019年, 公司云安全管理平台收入分别为141.85万、1418.59万、6723.83万元, 年复合增长率为588.48%; 虚拟化安全管理系统收入分别为2566.19万、6036.11万、8104.88万元, 年复合增长率为77.7%。

图33: 公司云安全业务收入高速增长



数据来源: 公司招股说明书、开源证券研究所

### 3、产品布局全面，传统赛道亦居领先地位

与国内同行业公司产品覆盖度相比, 公司是全领域覆盖的综合型网络安全厂商, 具有更为全面的产品布局。根据2020年3月31日安全牛发布的第七版中国网络安全行业全景图, 公司的产品线覆盖全部15个一级安全领域和71个二级细分领域。

域，是入围该全景图细分领域最多的网络安全企业。

图34: 奇安信是入围全景图细分领域最多的网络安全企业



资料来源: 安全牛

奇安信企业级防火墙获全球知名机构 Forrester 推荐。Forrester 发布《Now Tech: Enterprise Firewalls, Q1 2020》报告，共对全球 18 家主流的企业级防火墙品牌进行了技术及市场分析，中国品牌新华三、山石网科、华为和奇安信入选。

图35: 奇安信企业级防火墙获全球知名机构 Forrester 推荐

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

AWS	Huawei
Barracuda Networks	Juniper Networks
Check Point Software Technologies	Microsoft
Cisco	Optiv
F5 Networks	Palo Alto Networks
Forcepoint	<b>Qi An Xin</b>
Fortinet	Tufin
H3C	VMware
Hillstone Networks	Zscaler

资料来源: Forrester

此外，在中国移动公布 2020 年至 2021 年硬件防火墙产品集中采购(新建部分)中标候选人名单，奇安信旗下网神在标包三(需求数量最多的防火墙品类)以 20% 的份额入围，成为国内首家入围中国移动硬件防火墙集采项目的独立网络安全供应商。中国移动在此次防火墙招标项目中设置了功能测试、网络管理功能测试、SDN 测试、可靠性测试、性能测试、绿色节能测试等共计 40 个测试项目，是中国含金量最高的防火墙测试。奇安信首次参与测试，就在绝大部分项目中表现优异，充分体现了奇安信防火墙在产品性能、技术研发水平、创新能力等方面的领先优势。

**图36: 奇安信入围中国移动 2020-2021 年硬件防火墙集采项目**
**一、中标候选人的投标报价及中标情况:**
**标包2:**

第1中标候选人: 新华三技术有限公司, 投标报价28655941.95元 (不含税), 中标份额70%。

第2中标候选人: 华为技术有限公司, 投标报价35259284.70元 (不含税), 中标份额30%。

**标包3:**

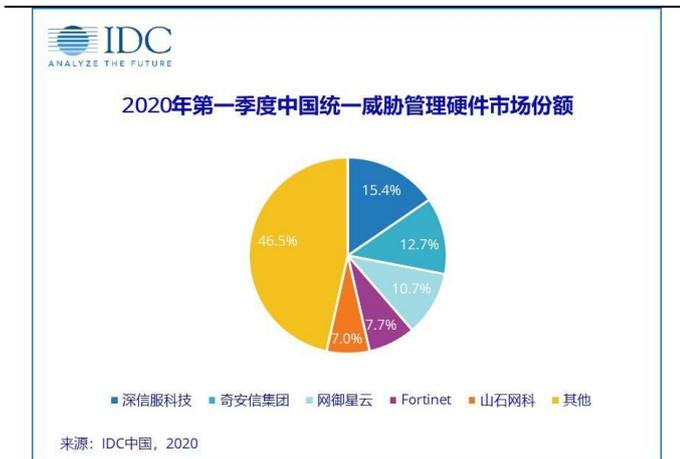
第1中标候选人: 华为技术有限公司, 投标报价22855560.00元 (不含税), 中标份额50%。

第2中标候选人: 新华三技术有限公司, 投标报价28894518.66元 (不含税), 中标份额30%。

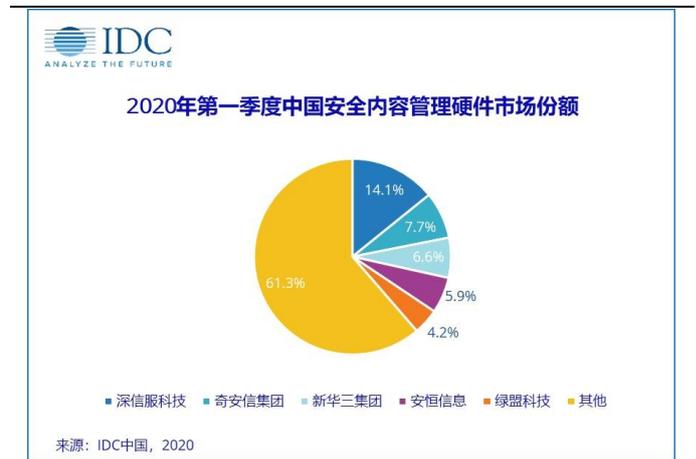
第3中标候选人: 网神信息技术 (北京) 股份有限公司, 投标报价22729980.00元 (不含税), 中标份额20%。

资料来源: 云技术

此外, 在统一威胁管理硬件及安全内容管理硬件等细分安全领域, 公司市场份额领先。

**图37: 公司在中国统一威胁管理硬件市场份额领先**


资料来源: IDC 中国

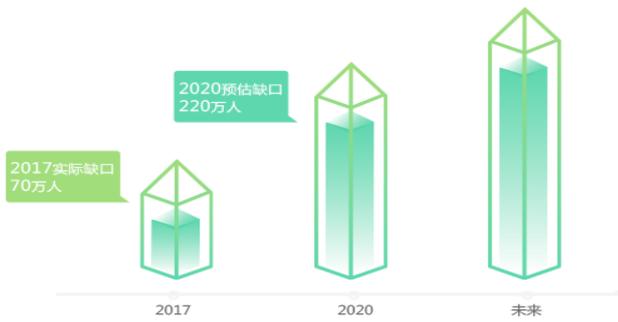
**图38: 公司在中国安全内容管理硬件市场份额领先**


资料来源: IDC 中国

## 4、紧抓行业需求, 打造精尖安全服务体系

中国网安行业人才缺口巨大。信息安全相关专业每年招生 2 万人, 但是总需求量超过 70 万人目前各类网络信息安全人才需求还将以每年 1.5 万人的速度递增, 到 2020 年需求将达 140 万人。与巨大的人才需求量相比, 目前国内的培养力量却显得极为薄弱, 全国只有 126 所高校设立了网络安全相关专业, 仅占 1200 多所理工院校的 10%。

图39: 2020年中国网安人才预估缺口 220万人



资料来源: 公司官网

图40: 中国网络安全人才需求和供给不匹配



资料来源: 公司官网

2018年公司人才培养基地&安全运营服务总部落地绵阳,规划总投资10亿元人民币。网络安全人才培养绵阳基地作为承载公司“以人为核心的安全运营服务”战略主体,于2018年3月29日在中国(绵阳)科技城正式启动,是公司包括安全运营服务总部、网络安全人才培养基地、网络空间安全军民融合创新中心绵阳分中心在内的三大战略之一,根据规划,总投资10亿元人民币,建成后人员规模将达到5000人,旨在为党政机构、军工保密和广大企事业单位提供网络安全运营服务和多层次的网络安全专业人才。2019年,公司培养了超过1500名的安全服务工程师。

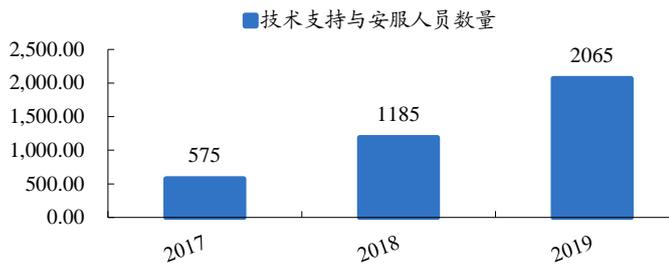
图41: 人才培养绵阳基地作为承载公司安全运营战略主体



资料来源: 公司官网

公司逐步建设了覆盖全国的应急响应服务体系,并在全国各地设立了应急响应团队,以形成公司大规模服务能力,为此公司快速扩张了人员规模并投入了大量的资金。2019年,公司共参与和处置了2000余起全国范围内的网络安全应急响应事件;共支持80余个客户的实网攻防演练工作,涉及27个部委、30家央企以及22个省市客户的实网攻防演练工作;参与了国家和地方重大活动网络安全保障任务50余次,包括投入超过1000人支撑新中国70周年国庆网络安全保障等。此外,公司决定在2020年12月正式将其7\*24小时的网络安全应急响应服务面向全社会推出,不局限于公司原有客户。

图42: 公司技术支持与安服人员数量已超过 2000 人



资料来源: 公司招股说明书

图43: 规模化、体系化投入攻防演习的攻击和防守



资料来源: 2019 年北京网络安全大会

## 5、盈利预测与投资建议

### 5.1、关键假设

**假设 1:** 依托公司已建立的技术优势、品牌优势及市场优势, 公司各项业务仍将保持高速增长;

**假设 2:** 公司逐渐建立了技术壁垒、品牌优势, 研发及销售费用投入收入占比有望逐渐降低;

**假设 3:** 第三方硬件产品在收入中的比例趋于稳定/略有降低, 公司综合毛利率有望实现稳中有升。

### 5.2、盈利预测与投资建议

公司是国内创新型网络安全领先厂商, 2017-2019 年公司营业收入复合增长率接近 96%, 依靠公司积累的技术优势、品牌优势及市场优势, 未来有望继续保持快速发展。同时, 随着公司逐渐步入高质量发展阶段, 盈利能力有望提升。我们预测公司 2020-2022 年归母净利润为-3.28、0.06、4.85 亿元, EPS 为-0.48、0.01、0.71 元/股, 当前股价对应 PS 为 17、12、9 倍, 公司 PE 高于行业可比公司平均水平, PS 与行业可比公司平均水平基本持平, 考虑公司为网络安全领军厂商, 正处于业务高速扩张期, 首次覆盖给予“买入”评级。

表8: 公司 PE 高于行业可比公司平均水平, PS 与行业可比公司平均水平基本持平 (截止 2020.9.17 收盘)

证券代码	公司简称	当前市值 (亿元)	归母净利润 (亿元)			PE			PS		
			2020E	2021E	2022E	2020E	2021E	2022E	2020E	2021E	2022E
688023.SH	安恒信息	184	1.32	1.83	2.44	139	101	75	14	10	7
300768.SZ	迪普科技	173	3.09	3.91	4.95	56	44	35	17	14	11
300454.SH	深信服	816	9.03	11.77	14.83	90	69	55	14	11	8
行业平均						95	71	55	15	12	9
688561.SH	奇安信	769	-3.28	0.06	4.85	-234	11952	158	17	12	9

数据来源: Wind、开源证券研究所 (迪普科技盈利预测均来源于 Wind 一致预期)

## 6、风险提示

1) 持续亏损风险。公司快速扩张了人员规模, 投入了大量资金, 产生了大量亏

损，目前由于规模效应仍未显现，公司存在持续亏损的风险。

**2) 商誉减值风险。**公司合并资产负债表中商誉的账面价值为 12.1 亿元，主要系非同一控制下控股合并网神股份、网康科技等企业所致。如果网神股份、网康科技等企业未来由于市场环境发生重大不利变化等原因导致业务开展未达到预期，可能导致商誉减值。

**附：财务预测摘要**

资产负债表(百万元)	2018A	2019A	2020E	2021E	2022E
<b>流动资产</b>	3991	3989	7084	5650	9735
现金	1646	1258	1753	2492	3340
应收票据及应收账款	619	1308	1589	1154	1649
其他应收款	936	367	1951	280	2012
预付账款	31	43	75	91	130
存货	611	749	1519	1423	2389
其他流动资产	148	264	197	211	215
<b>非流动资产</b>	2791	3166	3763	4295	4889
长期投资	454	392	459	498	530
固定资产	100	195	494	790	1060
无形资产	61	66	62	59	55
其他非流动资产	2176	2514	2748	2947	3243
<b>资产总计</b>	6782	7155	10847	9945	14624
<b>流动负债</b>	2396	1968	5949	5033	9172
短期借款	0	0	571	1156	1289
应付票据及应付账款	544	862	1194	1547	2040
其他流动负债	1852	1106	4184	2330	5842
<b>非流动负债</b>	109	146	119	126	127
长期借款	0	0	0	0	0
其他非流动负债	109	146	119	126	127
<b>负债合计</b>	2504	2114	6068	5159	9299
少数股东权益	-19	18	-17	-17	37
股本	149	578	680	680	680
资本公积	5817	6609	6609	6609	6609
留存收益	-1669	-2164	-2528	-2521	-1982
<b>归属母公司股东权益</b>	4297	5022	4796	4803	5288
负债和股东权益	6782	7155	10847	9945	14624

现金流量表(百万元)	2018A	2019A	2020E	2021E	2022E
<b>经营活动现金流</b>	-956	-1114	511	902	1687
净利润	-953	-553	-364	7	539
折旧摊销	86	140	114	214	334
财务费用	30	22	73	150	187
投资损失	-77	-196	-123	-139	-143
营运资金变动	-259	-609	810	671	770
其他经营现金流	216	82	-0	0	-0
<b>投资活动现金流</b>	-154	-219	-467	-605	-906
资本支出	100	283	470	547	545
长期投资	56	-13	-67	-40	-32
其他投资现金流	2	50	-65	-99	-393
<b>筹资活动现金流</b>	1884	927	2	-143	-186
短期借款	0	0	0	0	0
长期借款	0	0	0	0	0
普通股增加	127	428	102	0	0
资本公积增加	1791	792	0	0	0
其他筹资现金流	-34	-293	-100	-143	-186
<b>现金净增加额</b>	774	-406	-76	154	715

利润表(百万元)	2018A	2019A	2020E	2021E	2022E
<b>营业收入</b>	1817	3154	4635	6582	8827
营业成本	805	1365	1886	2580	3366
营业税金及附加	36	33	48	69	92
营业费用	800	1118	1483	1909	2295
管理费用	332	470	556	658	883
研发费用	818	1047	1390	1711	2118
财务费用	30	22	73	150	187
资产减值损失	-202	-3	-5	-7	-9
其他收益	176	243	320	360	499
公允价值变动收益	0	0	0	0	0
投资净收益	77	196	123	139	143
资产处置收益	0	0	0	0	0
<b>营业利润</b>	-953	-536	-355	11	537
营业外收入	1	2	2	1	2
营业外支出	1	5	6	6	9
<b>利润总额</b>	-953	-539	-359	7	530
所得税	-0	14	5	-0	-9
<b>净利润</b>	-953	-553	-364	7	539
少数股东损益	-81	-58	-36	1	53
<b>归母净利润</b>	-872	-495	-328	6	485
EBITDA	-917	-436	-273	209	851
EPS(元)	-1.28	-0.73	-0.48	0.01	0.71

主要财务比率	2018A	2019A	2020E	2021E	2022E
<b>成长能力</b>					
营业收入(%)	121.2	73.6	46.9	42.0	34.1
营业利润(%)	-35.1	43.8	33.7	103.2	4594.1
归属于母公司净利润(%)	38.4	-43.2	-33.7	-102.0	7443.5
<b>获利能力</b>					
毛利率(%)	55.7	56.7	59.3	60.8	61.9
净利率(%)	-48.0	-15.7	-7.1	0.1	5.5
ROE(%)	-22.3	-11.0	-7.8	0.2	10.3
ROIC(%)	-23.0	-11.6	-7.3	-0.1	8.0
<b>偿债能力</b>					
资产负债率(%)	36.9	29.5	55.9	51.9	63.6
净负债比率(%)	-37.1	-23.0	-23.7	-26.8	-37.7
流动比率	1.7	2.0	1.2	1.1	1.1
速动比率	1.3	1.5	0.9	0.8	0.8
<b>营运能力</b>					
总资产周转率	0.3	0.5	0.5	0.6	0.7
应收账款周转率	4.1	3.3	3.2	4.8	6.3
应付账款周转率	1.9	1.9	1.8	1.9	1.9
<b>每股指标(元)</b>					
每股收益(最新摊薄)	-1.28	-0.73	-0.48	0.01	0.71
每股经营现金流(最新摊薄)	-1.41	-1.64	0.75	1.33	2.48
每股净资产(最新摊薄)	6.32	7.39	6.91	6.92	7.63
<b>估值比率</b>					
P/E	-88.2	-155.4	-234.4	11951.5	158.4
P/B	17.9	15.3	16.4	16.4	14.8
EV/EBITDA	-82.1	-173.7	-277.4	361.6	88.1

数据来源：贝格数据、开源证券研究所

请务必参阅正文后面的信息披露和法律声明

## 特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

## 分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中的具体的推荐意见或观点有直接或间接的联系。

## 股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%~20%；
	中性（Neutral）	预计相对市场表现在 -5%~+5%之间波动；
	减持	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡	预计行业弱于整体市场表现。

备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。

## 分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

## 法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于机密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

本报告的版权归本公司所有。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

## 开源证券研究所

### 上海

地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层  
邮编：200120  
邮箱：research@kysec.cn

### 深圳

地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层  
邮编：518000  
邮箱：research@kysec.cn

### 北京

地址：北京市西城区西直门外大街18号金贸大厦C2座16层  
邮编：100044  
邮箱：research@kysec.cn

### 西安

地址：西安市高新区锦业路1号都市之门B座5层  
邮编：710065  
邮箱：research@kysec.cn