奇安信（688561）

全面布局主动防御体系，新兴安全优势明显

买入（首次）

2020 年 12 月 23 日

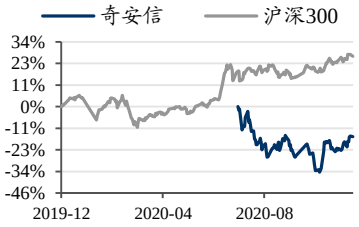
证券分析师 郝彪
执业证号：S0600516030001
021-60199781
haob@dwzq.com.cn

盈利预测与估值	2019A	2020E	2021E	2022E
营业收入（百万元）	3,154	4,481	6,324	8,732
同比（%）	73.6%	42.1%	41.1%	38.1%
归母净利润（百万元）	-495	-212	129	551
同比（%）	43.2%	57.1%	160.6%	328.1%
每股收益（元/股）	-0.73	-0.31	0.19	0.81
P/E（倍）	-161.89	-377.32	622.51	145.40

投资要点

- **高速成长的综合型体系化网安龙头，完成上规模阶段进入高质量发展阶段：**奇安信在 2014 年成立之初以打造实战化产品能力、协同联动产品体系及攻防对抗的安全服务体系为目标，采取“建设平台化研发能力、重视体系化安全交付、建立先发优势客户市场”的战略发展路径，制定“快速上规模”和“高质量发展”2 个 6 年的战略发展目标。2019 之前，处于“快速上规模阶段”的第一个 6 年，大量储备安全攻防人员，投入大量的资金建设四大研发平台、营销体系和安全运营服务体系。17 年至 19 年间，公司营业收入的年均复合增长率达到 95.98%，2019 年营收 31.54 亿元，收入规模处于国内第一梯队，四大研发平台、销售体系和应急响应服务体系建设也已基本完成，基本完成“快速上规模”的发展目标。2020 年开始将进入高质量发展阶段。
- **全面布局主动防护网安体系，先发优势明显：**公司以安全大数据为核心、威胁情报驱动的主动防护体系，满足党政军及关基行业客户从“被动防御”到“主动防御”体系的建设需求转变。叠加新 IT 架构场景需求，围绕上层的身份、数据、应用和行为等构建新的主动防御体系，公司时刻紧跟行业发展和攻防技术演进，推出了零信任、泛终端、新边界、云安全、态势感知等一系列具备攻防实战化效果的产品，在新细分赛道先发优势不断凸显。根据 IDC 的统计，奇安信态势感知、终端安全软件、安全资源池等新产品国内市占率第一，多款产品位居行业前列。
- **攻防实战为导向而非合规需求为导向，建设庞大的安全服务和应急响应团队：**攻防实战演习带动安全咨询、应急响应、安全托管服务等为主的安服需求，行业盈利模式正由软硬件产品销售向服务模式逐步转变。目前奇安信在全国 31 个省市建立了应急响应中心，技术支持及安服人员的人数超 2500 人，公司实战化能力而非合规需求导向也迎合了政企攻防实战演习需求，并带动公司产品高速增长。同时公司提出以“人+工具+数据+平台”的方式降低安全服务对人的依赖，大力布局安全自动化响应编排能力，为客户提供规划、建设、运行全链条的安全服务。
- **入列网安国家队，“PKS 体系”彰显优势。**2018 年中国电子升级“PK”体系为“PKS 体系”，(飞腾 CPU+麒麟操作系统+网络安全)，态“S”代表“可信计算”和“网络安全”。2019 年 5 月中国电子以 37 亿元战略入股奇安信，奇安信将安全技术与安全人才双向加持中国电子网络安全能力，双方深度融合，有望在“S”中占据重要地位。
- **盈利预测与投资评级：**预计公司 2020-2022 年营收分别为 44.81 亿元、63.24 亿元、87.32 亿元，归母净利润分别为-2.12 亿元、1.29 亿元、5.51 亿元。作为国内网络安全领域的龙头，目前仍处于相对高投入和前期布局阶段，费用高企，因此采取 PS 估值。选取国内外相关公司作为可比标的，高营收增速公司普遍享受高 PS，考虑公司在新兴安全领域的竞争优势、行业地位以及高成长速度，享受一定估值溢价，给予公司 2021 年产品和服务 18 倍 PS，对应目标市值约为 934.82 亿元，对应目标价 137.47 元，首次覆盖给予“买入”评级。
- **风险提示：**网络安全行业推进不及预期；资产减值风险。

股价走势



市场数据

收盘价(元)	117.90
一年最低/最高价	84.52/142.66
市净率(倍)	8.11
流通 A 股市值(百万元)	7773.24

基础数据

每股净资产(元)	13.85
资产负债率(%)	16.76
总股本(百万股)	679.62
流通 A 股(百万股)	69.24

相关研究

请务必阅读正文之后的免责声明部分

内容目录

1. 高速成长的综合型体系化网安产品方案及服务提供商 5
1.1. 体系化协同联动方案+全链条安全服务为主的业务体系 6
1.2. “快速上规模”目标完成，2020 年进入“高质量发展”阶段 8
1.2.1. “快速上规模”下的经营指标 8
1.2.2. 目前阶段“高质量发展”战略任务 11
2. 政策红利带动需求多点共振，服务化转型提升行业集中度 11
2.1. 政策红利带动行业需求多点共振，建设需求由等保合规进阶实战化演习 12
2.2. 行业服务化转型，头部集中趋势不变 18
3. 数据驱动安全，新赛道产品竞争力强 19
3.1. 基础架构安全体系：国内领先的零信任架构践行者和标准制定者 22
3.2. 新一代 IT 基础设施防护产品 25
3.2.1. 终端安全产品：国内市场份额第一 25
3.2.2. 私有云安全产品：国内市占率第一 27
3.2.3. 新一代智慧防火墙入围中国移动防火墙集采项目 28
3.2.4. 泛终端安全和云安全是主要收入增长贡献点。 30
3.3. 大数据智能安全检测与管控产品 31
3.3.1. 态势感知：国内市占率第一 31
3.3.2. 百场实战攻防磨炼利器“天眼” 32
3.3.3. 态势感知高速增长 33
4. 打造创新式全链条网络安全服务，在信创 PKS 体系中扮演重要角色 34
4.1. 网络安全服务：打造创新式全链条安全服务 34
4.2. 拥抱信创，有望在中国电子 PKS 体系中扮演重要角色 38
5. 盈利预测与估值 40
6. 风险提示 44

图表目录

图 1：奇安信发展历程 5
图 2：齐向东为公司控股股东和实控人 6
图 3：公司产品与服务体系示意图 6
图 4：网络安全产品主要产品 7
图 5：安全服务业务主要服务内容 8
图 6：过去 4 年营收高速增长 9
图 7：归母净利润亏损正逐步缩窄 9
图 8：公司营收构成（单位：亿元） 9
图 9：产品+服务的营收占比高 9
图 10：各产品毛利率 10
图 11：期间费用率逐年下降 10
图 12：过去三年员工总数增长一倍多（单位：人） 11
图 13：研发和技术支持及安服人员占据员工总数大半 11
图 14：等保 2.0 和等保 1.0 基本要求变化 13
图 15：等保 2.0 相比 1.0 法律效力提升 13
图 16：2019-2024 年中国 IT 安全支支出规模预测 14
图 17：2016-2021 年中国云安全市场规模及增速 14
图 18：2016-2021 年中国大数据安全市场规模及增速 14
图 19：2016-2021 年中国物联网安全市场规模及增速 14
图 20：2016-2021 年中国工业互联网安全市场规模及增速 14
图 21：态势感知是主动防御的安全大脑 15
图 22：攻防实战演习范围不断扩大 16
图 23：传统的网络安全架构 17
图 24：零信任架构 17
图 25：安全服务占比逐年提升 18
图 26：行业集中度在持续提升 18
图 27：《中国网络安全能力 100 强》榜首 19
图 28：安全牛中国网络安全百强企业榜首 20
图 29：零信任产品架构图 22
图 30：奇安信零信任安全解决方案 23
图 31：子公司网神等制定的零信任标准获得立项 24
图 32：基础架构安全产品营收 24
图 33：天擎终端安全管理系统功能展示 25
图 34：终端安全产品结构 26
图 35：2019 年终端安全软件市场份额 27
图 36：安全资源池国内市占率第一 28
图 37：智慧防火墙产品架构图 28
图 38：中国移动防火墙集采中标详情，奇安信中标份额为标 3 的 20% 29
图 39：新一代 IT 基础设施防护产品营收 30
图 40：奇安信在 IDC2019 年态势感知厂商评估中拍第一 32
图 41：新一代威胁感知与响应系统（“天眼”）产品架构图 32
图 42：大数据智能安全检测与管控产品营收 33

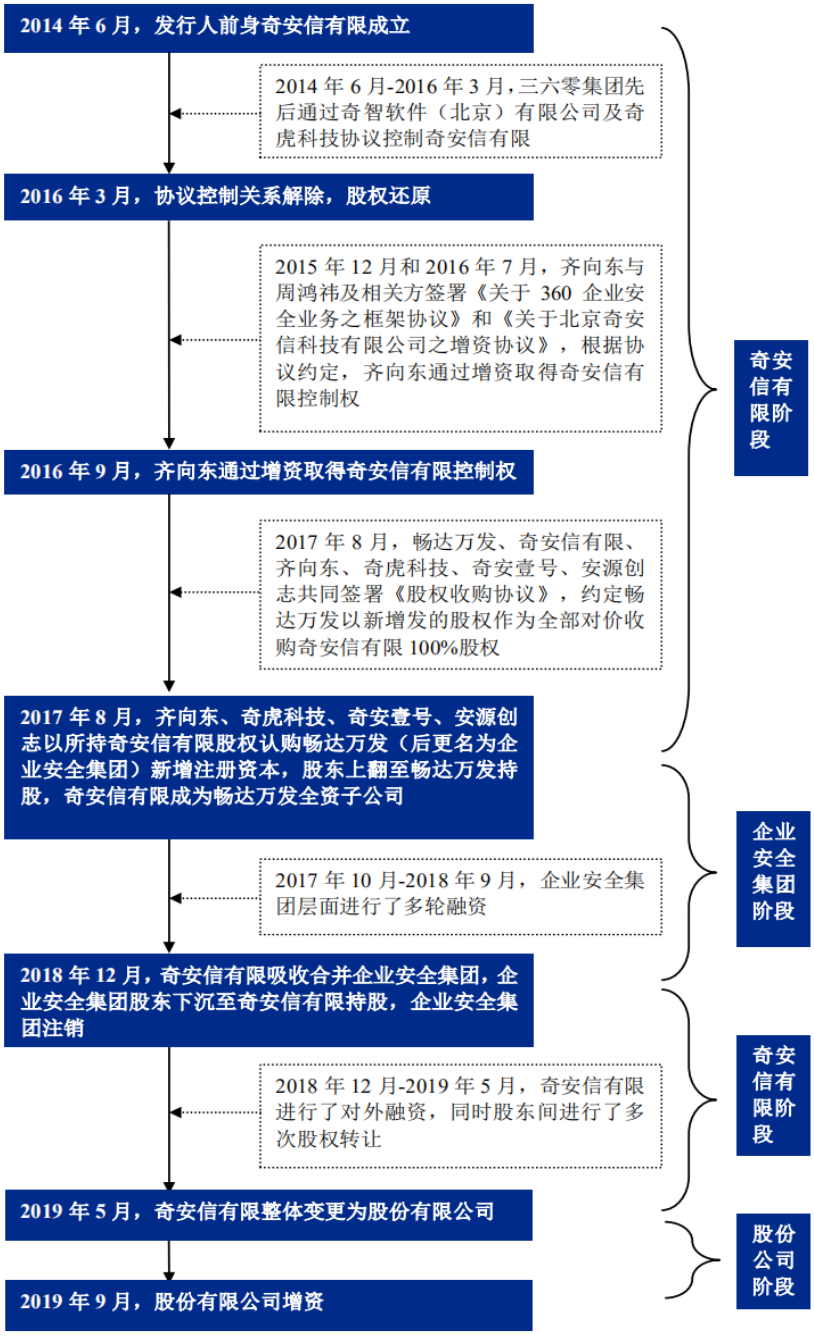
图 43：领跑国内安全资讯市场.....35
图 44：人才培养基地布局图.....37
图 45：2019 年信安全服务企业排名第一.....37
图 46：奇安信网神终端安全管理系统在麒麟 v10 上运行状况.....38
图 47：在新的 PKS 体系中，奇安信有望在 S 环节占据重要地位.....39
图 48：营收拆分与预测（单位：百万元）.....40
图 49：安恒信息上市以来 PS（TTM）（截止 2020.12.20）.....42
图 50：Palo Alto 过去 9 年营收和增速.....42
图 51：Palo Alto 过去 9 年 PS（TTM）（截止 2020.12.20）.....42
图 52：Crowdstrike 过去 4 年营收和增速.....43
图 53：Crowdstrike 上市以来 PS（TTM）（截止 2020.12.20）.....43
图 54：Okta 过去 4 年营收和增速.....43
图 55：Okta 上市以来 PS（TTM）（截止 2020.12.20）.....43

表 1：近年来网络安全相关的政策密集发布.....12
表 2：公司产品市场排名情况.....20
表 3：公司营收中新老客户贡献收入情况.....21
表 4：基础架构安全产品主要收入贡献产品.....25
表 5：新一代 IT 基础设施防护产品重要产品收入.....31
表 6：以态势感知为代表的大数据安全产品高速增长.....34
表 7：安全运营提供的多类型服务.....36
表 8：行业可比标的估值（截至 10 月 11 日）.....42

1. 高速成长的综合型体系化网安产品方案及服务提供商

起始于 360 政企安全创业团队，5 年入列网安国家队。公司成立于 2014 年，原系三六零集团控股子公司，主要负责政府企业安全市场，2016 年 7 月从三六零集团拆分出来，成为独立运营的 360 企业安全集团，共享 360 品牌，但技术独立。2019 年 4 月 30 日更名为奇安信集团。2019 年 5 月 10 日，360 转让所有股权，中国电子出资 37.31 亿元获得奇安信 22.59%股权，成为奇安信第二大股东，**奇安信正式入列网络安全国家队。**

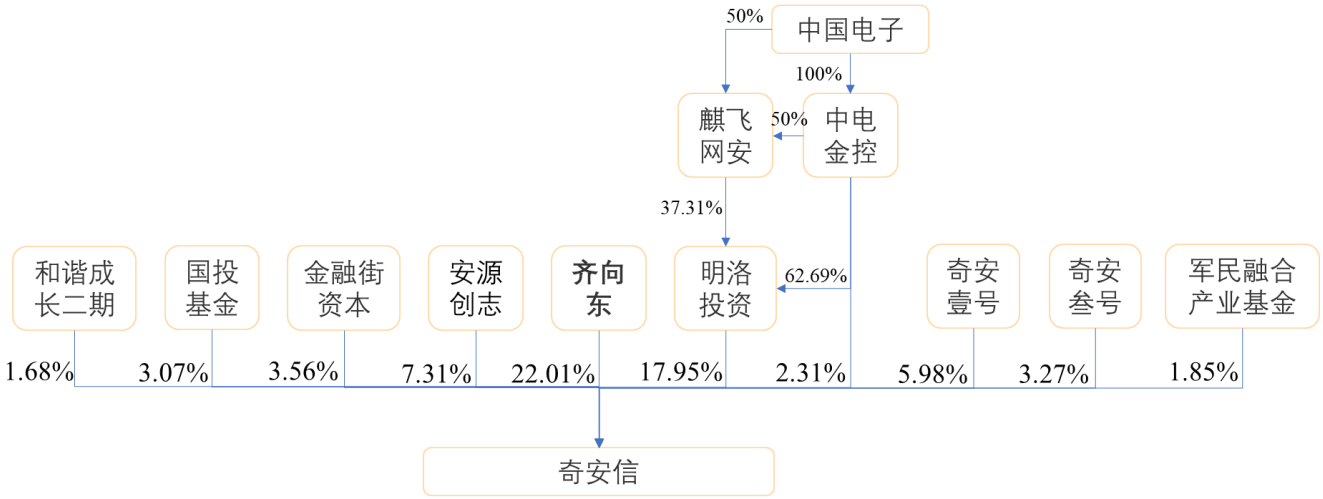
图 1：奇安信发展历程



数据来源：招股说明书，东吴证券研究所

董事长齐向东为实控人，中国电子为第二大股东。奇安信实际控制人为董事长齐向东，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 10.58%的股份，合计控制公司 32.59%的股份，为公司控股股东和实际控制人。中国电子通过子公司明洛投资和中电金控持有 20.26%股份，为第二大股东。

图 2：齐向东为公司控股股东和实控人



数据来源：Wind，东吴证券研究所

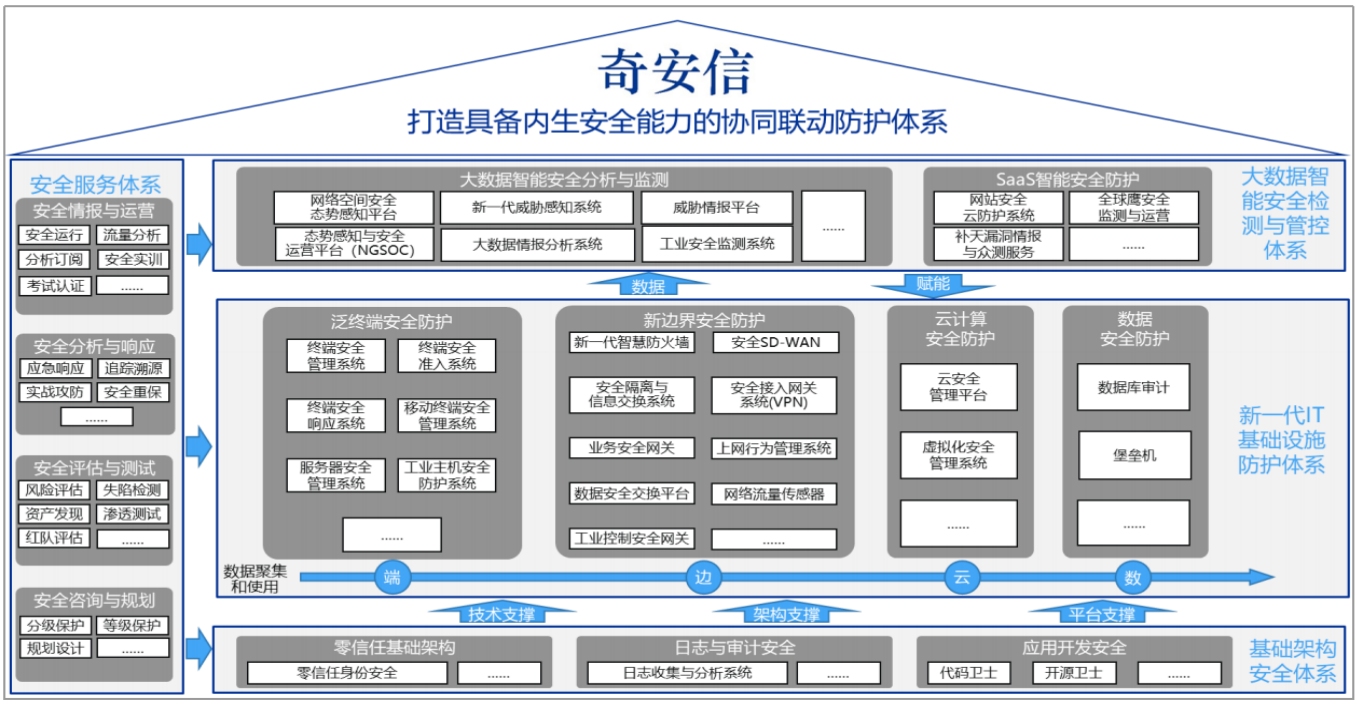
1.1. 体系化协同联动方案+全链条安全服务为主的业务体系

政企客户为主，国内领先的网安综合型供应商。奇安信目前主要目标市场是国家安全、行业安全、商业企业安全市场。主营业务为向政府、企业用户提供新一代企业级网络安全产品和服务，客户范围覆盖大多数中央政府部门、中央企业和金融、能源、医疗、运营商、教育、交通等行业。凭借持续的创新研发和以实战攻防为核心的安全能力，已发展成为国内领先的基于安全大数据、人工智能和安全运营技术的网络安全供应商。

具备体系化交付能力和协同联动属性的实战化网络安全产品和全链条的安全服务是公司的核心竞争力。公司成立之初就致力于打造协同联动的安全防护产品能力、产品体系及实战化的安全服务体系，目前公司为政企客户提供的主要产品和服务为：网络安全产品、网络安全服务、硬件及其他。

图 3：公司产品与服务体系示意图

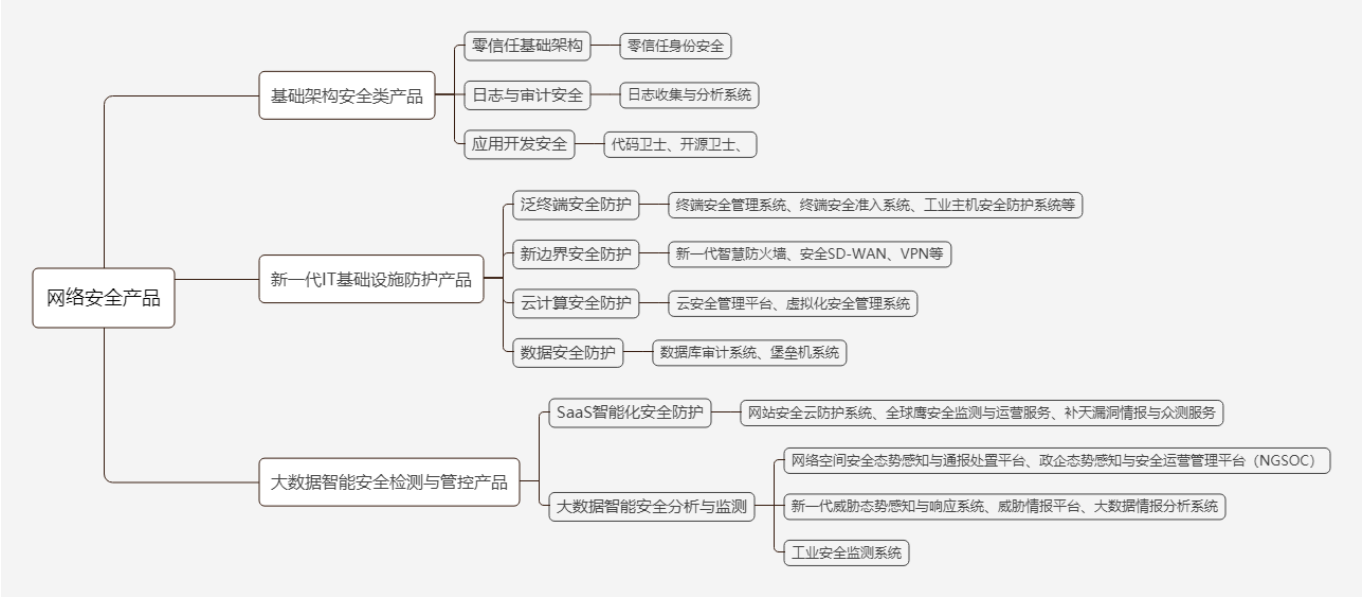
公司产品与服务体系示意图



来源：招股说明书，东吴证券研究所

安全产品业务：覆盖政企行业网络安全的各细分领域，具体又包括三大类别：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。

图 4：网络安全产品主要产品



数据来源：招股说明书，东吴证券研究所

安全服务业务：基于“安全大数据驱动安全”技术理念，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，提供规划阶段的服务——“安全咨询与

规划”，运行阶段的服务——“安全分析与响应”；同时，将实网攻防和数据运营等技术应用于运行阶段，改造了传统的安全服务，形成自有特色的“安全评估与测试服务”和“安全情报和运营”服务。

图 5：安全服务业务主要服务内容



数据来源：招股说明书，东吴证券研究所

硬件及其他业务：系公司在网络安全性质的系统集成项目中为客户提供的第三方硬件采购、实施（如需）等业务。在部分项目中，公司提供的网络安全解决方案为大型政企客户信息化改造项目中的组成部分，也承担为此类客户配套外采其他系统集成硬件产品并销售给对方的业务。

1.2. “快速上规模”目标完成，2020 年进入“高质量发展”阶段

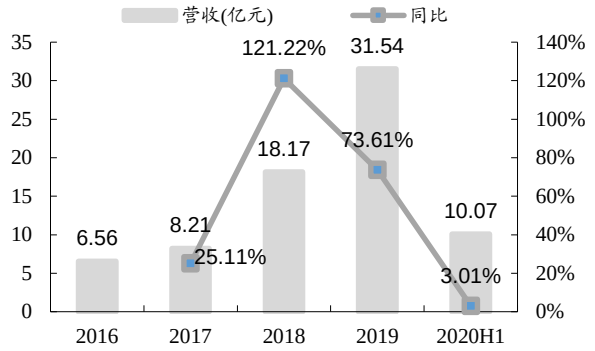
2019 年末“快速上规模”已基本完成。公司在 2014 年成立之初就以打造协同联动的安全防护产品能力、实战化防御效果的产品体系及实战化攻防能力的安全服务体系为目标，采取的是“建设平台化研发能力、重视体系化安全交付、建立先发优势客户市场”的战略发展目标和布局。围绕这个发展目标和布局，公司设置了两个阶段的发展目标，分别为“快速上规模”及“高质量发展”。2019 年之前，大量扩张人员规模，投入大量的资金建设四大研发平台、营销体系和应急响应服务体系。截至 2019 年末，公司营收 31.54 元，收入规模已经处于国内第一梯队，四大研发平台形成了平台化及模块化的研发能力，销售体系和应急响应服务体系建设也已基本完成，所以目前公司基本完成了“快速上规模”的发展目标。

1.2.1. “快速上规模”下的经营指标

“快速上规模”表现一：营收高增长。2017 年-2019 年公司营收分别为 8.2 亿元、18.17 亿元和 31.54 亿元，年均复合增长率为 95.98%，实现了高速增长。2017-2019 年归

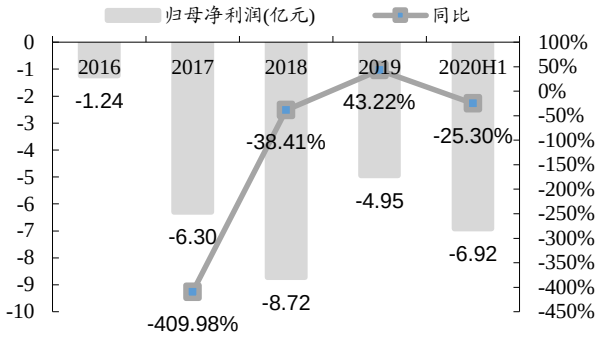
母净利润分别为-6.3 亿元、-8.72 亿元、-4.95 亿元，仍处于亏损状态，亏损主要原因是公司高研发投入和人员快速扩张的发展模式带来的高费用支出。

图 6：过去 4 年营收高速增长



数据来源：Wind，东吴证券研究所

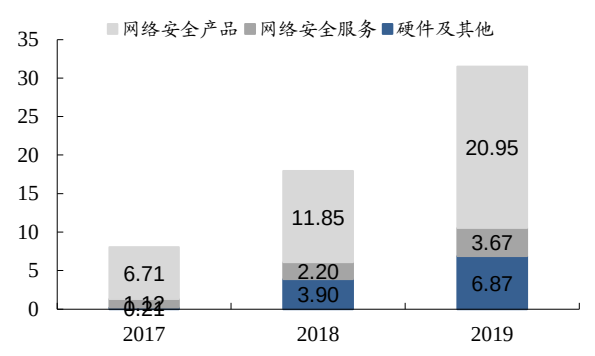
图 7：归母净利润亏损正逐步缩窄



数据来源：Wind，东吴证券研究所

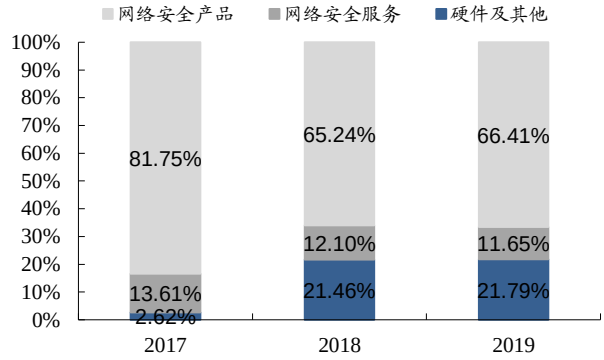
实战化防护效果的产品体系+全链条安全服务为主要营收来源。实战化防护效果的安全产品及全链条覆盖的安全服务是公司的主营业务，2017-2019 年产品+服务业务的合计占比分别为 95.36%、78.34%、78.06%。其中，网络安全产品占比从 2017 年的 81.75%下降为 2019 年的 66.41%，网络安全服务的占比较为稳定，在 12%左右。2020 年前三季度，公司安全服务收入达到 15%以上，安全服务业务成为营收新引擎之一。近几年，由于政企信息化改造速度加快，公司客户信息化改造的综合需求不断增加，参与此类项目的数量和规模增长较快，第三方安全集成（硬件及其他）营收占比从 2017 年的 2.62%提升至 21.79%，随着公司精细化治理效果不断凸显，预期公司的第三方集成业务占比将呈现逐渐收敛趋势。

图 8：公司营收构成（单位：亿元）



数据来源：Wind，东吴证券研究所

图 9：产品+服务的营收占比高

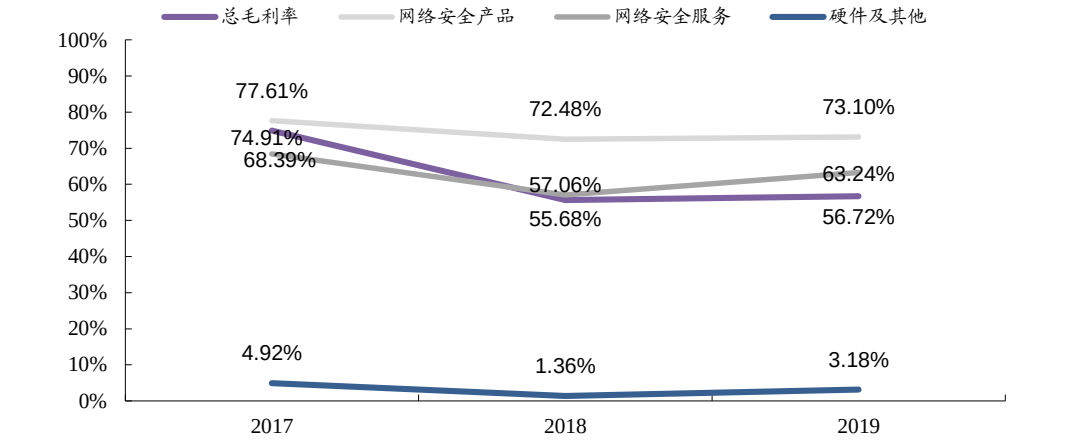


数据来源：Wind，东吴证券研究所

安全产品和服务毛利率稳中有升，安全集成业务拉低公司毛利率。2017-2019 年公司毛利率分别为 74.91%、55.68%、56.72%，呈下降趋势，主要是由于公司毛利率较低的硬件及其他业务收入在 2018 年和 2019 年的增长幅度相对较高，带动期间毛利率水平下

降。安全产品毛利率相对较为稳定，2017-2019 年安全产品毛利率分别为 77.61%、72.48%、73.10%，安全服务毛利率分别为 68.39%、57.06%、63.24%。

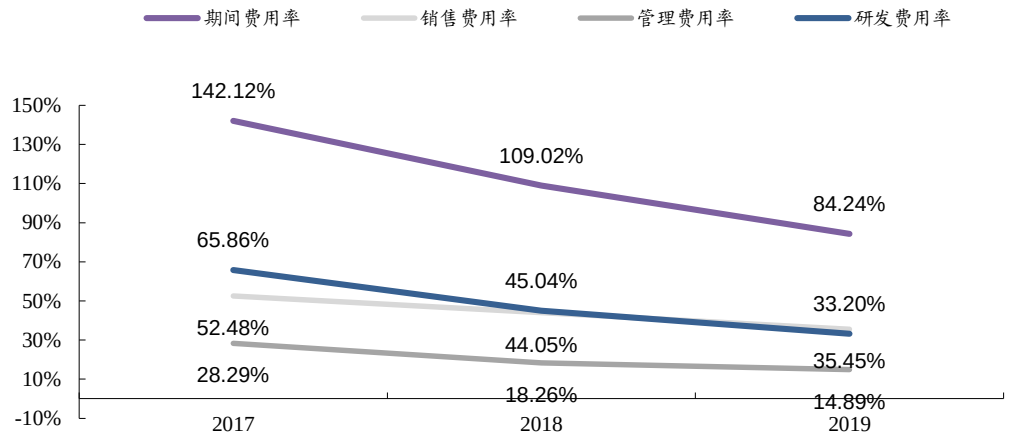
图 10：各产品毛利率



数据来源：Wind，东吴证券研究所

上规模战略表现二：高研发和销售投入。2017—2019 年公司期间费用率分别为 142.12%、109.02%、84.24%，由于公司投入大量资源进行四大研发平台的创新和新赛道业务拓展，导致研发费用和销售费用投入大，带动整体费用率高企。虽然随着公司规模效应的显现，收入增速高于费用增速，期间费用率呈现逐年下降的趋势，但仍高于行业平均水平，主要原因是公司提前布局四大研发平台，不断加大安全运营投入。目前公司的四大研发平台和销售渠道陆续完善，随着营收体量不断变大，预计公司的研发和销售费用率会逐步控制在一个相对稳定的范围内，中长期具备研发费用占比收窄趋势。

图 11：期间费用率逐年下降

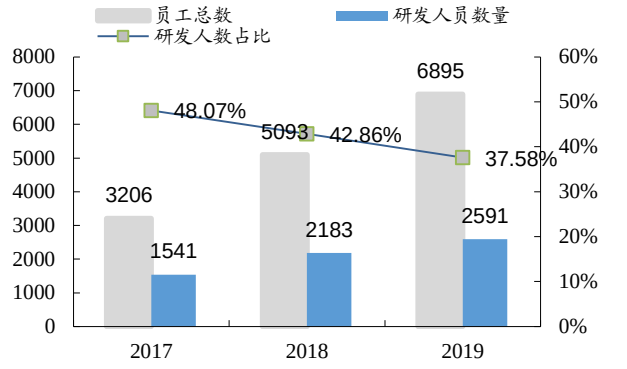


数据来源：Wind，东吴证券研究所

上规模战略表现三：快速扩张的员工队伍和覆盖全国的应急响应服务体系。2017-2019 年公司员工总数为 3206、5093、6895 人，过去三年员工总数实现翻倍增长。截止 2019 年末，研发人员 2591 人，占比 37.58%。同时，公司建立了覆盖全国 31 个省市自治区的应急响应中心，技术支持及安全服务人员 2545 人，占比 36.91%，向客户（包含已有和潜在客户）提供应急响应技术服务。销售人员 1097 人，占比 15.91%，形成了覆

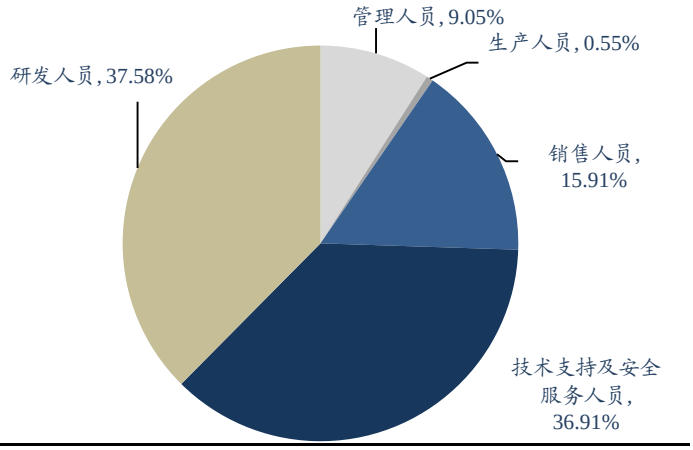
盖全国的销售网络。目前公司处于第二个六年的“高质量发展”阶段，人员增速保持在稳定状态内，开始针对员工进行组织优化和末尾淘汰制，数字化管理和经营中长期会提升人效预期。

图 12：过去三年员工总数增长一倍多（单位：人）



数据来源：Wind，东吴证券研究所

图 13：研发和技术支持及安服人员占据员工总数大半



数据来源：招股说明书，东吴证券研究所

1.2.2. 目前阶段“高质量发展”战略任务

“高质量发展”阶段将围绕“提效降本”。2020 年初开始，公司进入“高质量发展”阶段，将主要围绕“提效降本”的目标，主要在研发端和销售端以及公司管理层面采取一些更优的策略和举措。**研发端，**重点推动“建研发平台”到“用好研发平台”的转变，一方面，不依靠人员扩展，推进综合元效管理和考核，推动研发人员利用四大研发平台的技术成果孵化新产品，拓展新市场；另一方面，利用四大平台推动“模块化”策略，将更多产品功能、组件、技术转化为标准模块和平台，进一步降本增效。在未来新赛道产品的研发周期上会更快的投入市场，确保先发优势地位。**市场销售端，**一方面，在以往党政军部委客户基础上，向涉及民生的重点基础行业（能源、金融、医疗为甚、运营商等）为重点拓展，提升商业市场份额；另一方面，营销体系向二三线城市和企业级市场渗透，渠道建设同步加速，进一步提升渗透率。

公司预计在收入达到 44-46 亿元时可实现盈亏平衡。随着公司布局的完善，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”的趋势，未来实现盈利高速增长可期。根据公司管理层的测算，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，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。

股权激励留住核心人才。公司在上市 4 个月内，完成了核心员工股权激励动作，预期针对留住核心员工并激发积极性将产生重要作用，赋予未来发展潜力。

2. 政策红利带动需求多点共振，服务化转型提升行业集中度

2.1. 政策红利带动行业需求多点共振，建设需求由等保合规进阶实战化演习

政策推动行业景气度提升。近年来随着国内外网络安全事故的频发，我国政府不断提高对网络安全的重视。2013 年以来先后设立了国家安全委员会、中央网络安全和信息化委员会。2017 年 6 月 1 日，《网络安全法》正式发布，其作为我国网络安全的基本法，使得整个行业进入合法的时代，真正做到有法可依。近两年来，与《网络安全法》相配套的等保 2.0、《密码法》等也都陆续发布或者在立法阶段，法律将渗透在网络安全的各个分支和各个行业，提高政府、企业在网络安全方面的投入，必将推动整个行业往更为规范和成熟的方向发展。与此同时，合规需求和攻防需求也将带动整个行业进入新的加速成长阶段。

表 1：近年来网络安全相关的政策密集发布

时间	事件	内容
2020 年 7 月	全国人大发布《数据安全法（草案）》	确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施。
2020 年 4 月	国家互联网信息办公室等 12 部门正式发布了《网络安全审查办法》	于今年 6 月 1 日起实施。网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险，包括金融、电信、交通、能源等 10 多个行业的网络系统。
2020 年 1 月	全国人大通过的《密码法》正式施行	规定使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估，并对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，于 2020 年 1 月 1 日正式实施。
2019 年 5 月	公安部正式发布《网络安全等级保护条例》即等保 2.0	注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。
2019 年 3 月	国务院国资委修订印发了《中央企业负责人经营业绩考核办法》	条例对政府机关，国家行业主管或监管部门，能源、电信、交通等行业，明确关键信息基础设施范围，规定运营者安全保护的权利和义务及其负责人的职责。
2019 年 3 月	《关键信息基础设施安全防护条例》纳入《国务院 2019 年立法工作计划》	对关键信息基础设施安全提出强制性要求。
2019 年 3 月	《个人信息保护法》已列入本届立法规划	整合、修改和补充原有的法律规范，消除其间的矛盾和混乱，建立规范、系统的法律体系，能明确基本原则、基本制度、基本行为规范和法律责任。
2018 年 12 月	国务院国资委修订印发了《中央企业	条例自 2019 年 4 月 1 日起施行。条例对政府机关，国家行业主

	负责人经营业绩考核办法》	管或监管部门，能源、电信、交通等行业，明确关键信息基础设施范围，规定运营者安全保护的权利和义务及其负责人的职责。
2018 年 4 月	国务院国资委修订印发了《中央企业负责人经营业绩考核办法》	条例对政府机关，国家行业主管或监管部门，能源、电信、交通等行业，明确关键信息基础设施范围，规定运营者安全保护的权利和义务及其负责人的职责。
2017 年 6 月	《中华人民共和国网络安全法》正式施行	为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。

数据来源：网信办官网，东吴证券研究所

等保 2.0 正式实施，重点纳入新保护对象。2019 年 5 月 13 日等保 2.0 国家标准正式发布，并于 2019 年 12 月 1 日开始实施。等保 2.0 对等保对象和保护内容进行了扩充，在 1.0 的基础上，注重全方位主动防御、动态防御、整体防控和精准防护，加强对云计算、大数据、物联网、移动互联网和工业控制信息系统等保护对象的安全要求。

图 14：等保 2.0 和等保 1.0 基本要求变化

	等保1.0	等保2.0	
保护内容	定级、备案、建设整改、等级测评和监督检查等五个规定	定级、备案、建设整改、等级测评和监督检查等五个规定的基础上，增加风险评估、安全监测、通报预警，案事件调查、数据防护、灾难备份、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施	**受益产品：**安全管理（态势感知）、数据安全、安全服务（合规评价、风险评估）
保护对象	一个基本要求： 1）网络和信息系统	安全通用要求和安全扩展要求： 1）安全通用要求 2）云计算安全扩展要求 3）移动互联安全扩展要求 4）物联网安全扩展要求 5）工业控制系统安全扩展要求	**新增市场规模：** 528.4亿元-1321亿元
监管对象	体制内	全社会	

数据来源：网信办官网，东吴证券研究所

图 15：等保 2.0 相比 1.0 法律效力提升

	等保1.0	等保2.0
名称	信息(系统)安全等级保护	网络安全等级保护
顶层规范性文件	计算机信息系统安全保护条例 (行政法规)	网络安全法 (法律)
核心体系稳健	信息安全等级高保护管理办法 (部门规范性文件)	网络安全等级保护条例 (行政法规)
配套标准	以GB/T 22239/28448等为核心的信息系统安全等级保护标准及其他配套标准	以修订GB/T 22239/28448等为核心的网络安全等级保护标准及其他配套标准

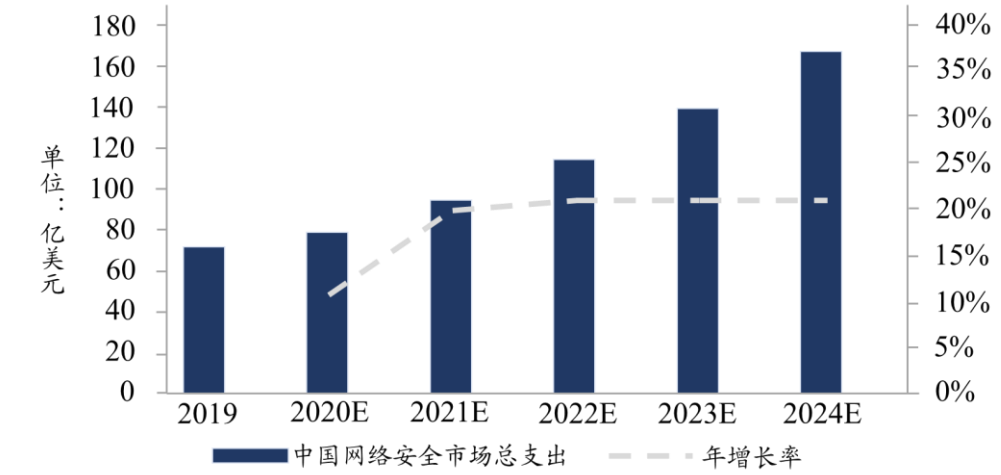
数据来源：网信办官网，东吴证券研究所

新技术的应用给安全市场带来新的需求。在传统网络安全防护时代，由于网络环境（互联网、隔离或非隔离内网）、用户终端（PC 为主）、政企应用（OA、CRM、ERP 为主）等相对简单，针对信息化的安全防护更加注重网络边界的保护，产品主要以针对边界防护隔离的硬件产品和针对主机及应用系统的软件形态的产品为主。随着云计算、大数据等新兴技术的广泛应用，用户终端（PC 向移动终端、IoT 终端、工业主机等泛终端形态扩展）、网络环境（云、端带来新边界）、应用和数据（类型和复杂度增加）的变化等对安全防护带来了新的需求，围绕上层的身份、数据、应用和行为等需要构建新的防御体系，新的产品细分赛道不断涌现。

新兴安全领域增速高于行业整体增速，呈加速发展态势。在政策和数字化经济转型的驱动下，我国网络安全行业仍将继续保持较快的增长。根据 IDC 预测，2020 年中国网络安全市场总体支出将达到 78.9 亿美元，较 2019 年同比增长 11.0%，到 2024 将增长至

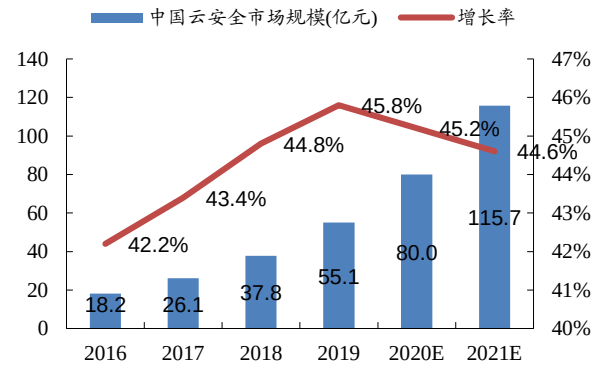
179.0 亿美元，2020-2024 年 CAGR 为 18.7%。而根据赛迪咨询的预测，2020 年云安全、大数据、物联网安全、工控安全等新兴安全领域的市场规模分别为 80.0、51.5、195.1、168.7 亿元，同比增速分别为 45.8%、33.8%、45.2%、32.2%，高于网络安全市场的总体增速；2020 年将达到 495.3 亿元，同比增速为 42.7%，各增速均高于行业增速。

图 16：2019-2024 年中国 IT 安全支支出规模预测



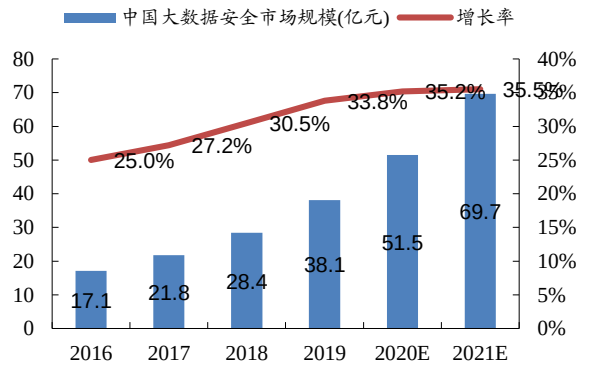
数据来源：IDC，东吴证券研究所

图 17：2016-2021 年中国云安全市场规模及增速



数据来源：赛迪咨询，东吴证券研究所

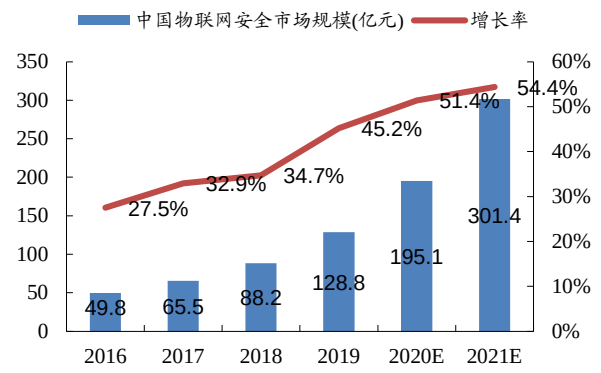
图 18：2016-2021 年中国大数据安全市场规模及增速



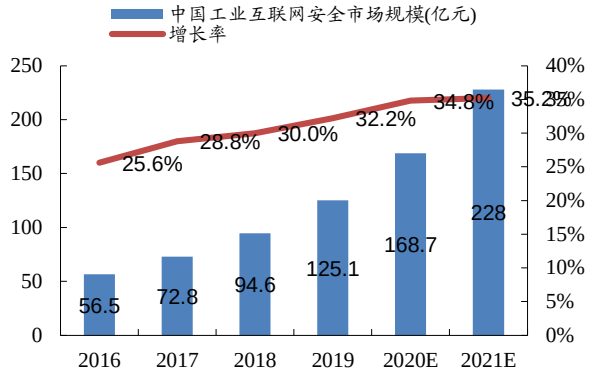
数据来源：赛迪咨询，东吴证券研究所

图 19：2016-2021 年中国物联网安全市场规模及增速

图 20：2016-2021 年中国工业互联网安全市场规模及增速



数据来源：中国信通院，东吴证券研究所



数据来源：赛迪咨询，东吴证券研究所

客户的安全建设需求从被动防御向主动防御阶段转变。近年来，网络攻击由过去黑客炫技的个人行为，发展成有组织的犯罪或者攻击行为，呈现手段专业化、目的商业化、源头国际化及载体移动化的趋势。传统的以安全硬件为核心的被动防御体系无法抵御当前的网络攻击，整个行业正在由被动防护向主动防御模式转变。奇安信具备以安全大数据为核心的、威胁情报驱动的云-终端-边界网关协同联动的防护体系，并拥有态势感知和安全运营的体系化方案，可以满足客户主动防护体系建设的中长期需求。

以安全大数据为核心的态势感知体系是主动防御体系的安全大脑。随着互联网的迅猛发展，网络安全态势感知应运而生，其工作原理是对网络环境中引起网络态势发生变化的安全要素信息进行获取、理解，进而评估网络安全的状况，预测其发展趋势，并以可视化的方式展现给用户，帮助用户实现相应的安全决策与行动，从而实现积极主动的动态安全防御。被动防御时代以边界防护为主，防火墙是最重要的产品，主动防御时代安全大脑是防御体系中最核心的组成部分，而态势感知充当的就是安全大脑的角色。

图 21：态势感知是主动防御的安全大脑



数据来源：环球网，东吴证券研究所

网络态势感知成为国家重点推进工程。2016 年 4 月 19 日，习近平总书记在网信工作座谈会上发表讲话，第一次提到“全天候全方位感知网络安全态势”，国家把态势感知的建设放到了十分重要的位置。2016 年 12 月 15 日，国务院发布的十三五国家信息化规划中，将“健全网络安全保障体系”作为十大任务之一，明确提出要“全天候全方位感知网络安全态势”。在 2017 年的 2·17 国家安全工作座谈会中，习近平总书记强调“要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护”。这充分表明，党中央和国务院均将态势感知作为国家重点工程推进。

建设需求由等保合规进阶实战化演习。网络安全的本质不是被动防御，是主动防御对抗。《网络安全法》规定关键信息基础设施的运营者应制定网络安全事件应急预案，并定期进行演练，自此实战攻防演练成为网络安全建设的重要一环。网络安全实战攻防演练专项行动已成为一年一度的惯例，同时所涉及的单位和规模持续扩大。攻防实战演练已成为检验参演单位网络安全综合防御水平的“试金石”和提升网络攻击应对能力的“磨刀石”。在攻防实战演习的带动下，机构对网络安全的需求也从被动构建向业务保障刚需升级。

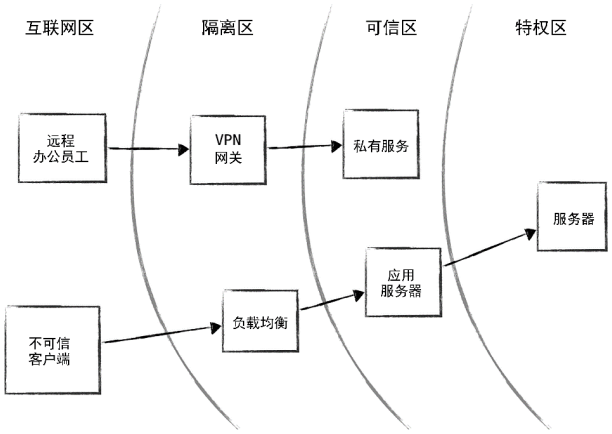
图 22：攻防实战演习范围不断扩大



数据来源：人人云图，东吴证券研究所

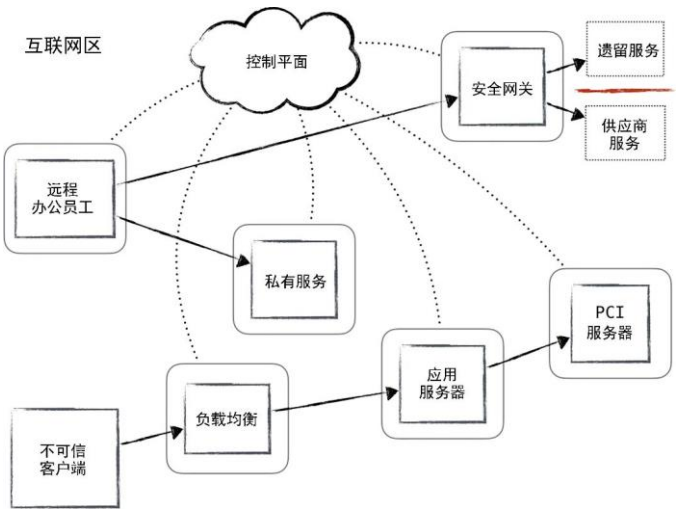
零信任安全架构正逐步取代传统基于网络边界的安全架构。传统的安全架构通过边界防护设备划分出企业内网和外网，并以此构建企业安全体系，内网用户默认享有较高的网络权限，而外网用户接入内网都需要通过 VPN。随着云计算、大数据、物联网、移动互联网等技术的兴起，带来日趋开放和复杂的网络边界，灵活的移动办公，内网边界也日趋复杂与模糊，让基于边界的安全防护逐渐失效，来自企业外部的欺诈和内部的信息泄露造成的损失逐年剧增，一种基于“零信任框架模型”的网络安全架构由此诞生。零信任体系对外部公共网络和本地网络的设备在默认情况下都不会授予任何特权，用户无论在哪里，无论什么时间，只有使用通过受控设备、通过身份认证，且符合“访问控制引擎”中的策略要求，通过专用访问代理才能访问特定的公司内部资源。

图 23：传统的网络安全架构



数据来源：《零信任网络》，东吴证券研究所

图 24：零信任架构



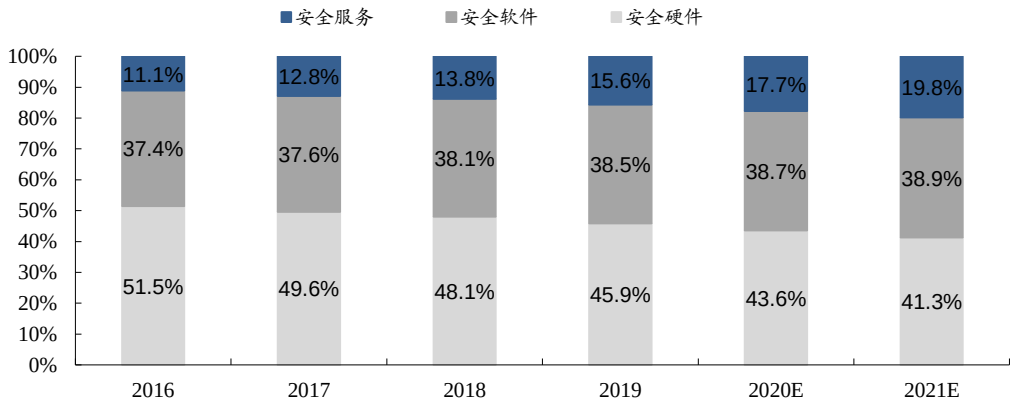
数据来源：《零信任网络》，东吴证券研究所

零信任的核心思想是身份控制：网络边界内外的任何访问主体（人/设备/应用），在未经过验证前都不予信任，需要基于持续的验证和授权建立动态访问信任，其本质是以身份为中心进行访问控制。

2.2. 行业服务化转型，头部集中趋势不变

网络信息安全市场持续向服务化转型，安全市场结构进一步优化。在网络信息安全产业发展过程中，大多数是由合规需求驱动的，而近年来的灾难性攻击表明网络风险是重大威胁，网络威胁正向多样化和复杂化的方向演化，传统的单一安全产品的模式已经很难满足客户的安全防护需求。企业开始把安全视为一项重要的商业风险，以风险评估、安全管理咨询、安全应急响应、安全托管服务等为主的安全服务越来越受到用户的青睐。随着虚拟化及云理念渗透，云化产品快速发展，安全服务的价值得到认可，威胁监测、威胁情报等新兴模式逐步试点应用，行业盈利模式将由软硬件产品销售向服务模式逐步转变。赛迪咨询数据显示，2016 年以来，中国安全服务的支出占比提升了 6 个多点。

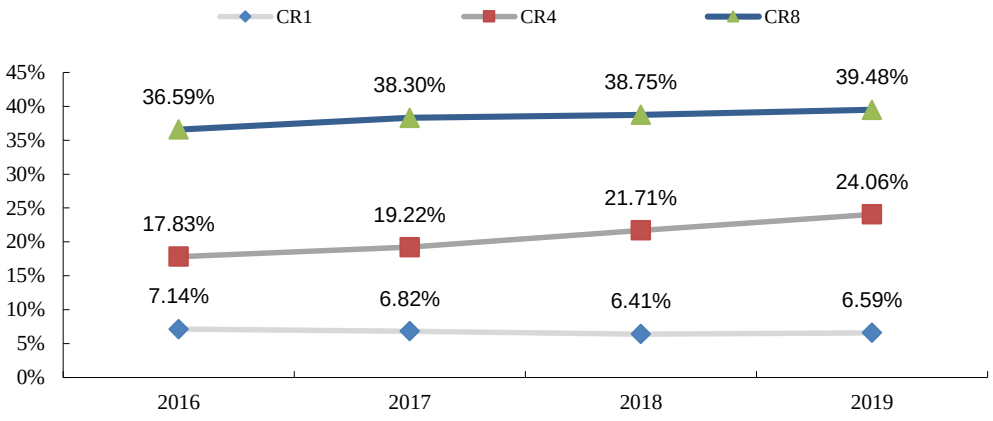
图 25：安全服务占比逐年提升



数据来源：赛迪咨询，东吴证券研究所

行业竞争格局仍然分散，龙头集中趋势明显。网络安全细分领域多，行业竞争格局分散，目前单一厂商的市场份额不超过 10%，但根据中国网络安全产业联盟的统计数据，2016-2019 年，国内网安行业 CR4 和 CR8 企业的市占率不断提升，产业正逐步往行业头部集中。目前行业内领先企业无论是技术创新力度还是产品研发能力不断提升，市场正不断的向这些具有丰富产品线和规模化服务能力的厂商汇聚，同时行业由单一产品采购逐步变为综合方案需求和安全运营能力输出，龙头公司优势将不断强化，正向反馈也带动这些厂商的竞争力越来越强，因此我们预计未来市场集中度提升的趋势仍将继续。

图 26：行业集中度在持续提升

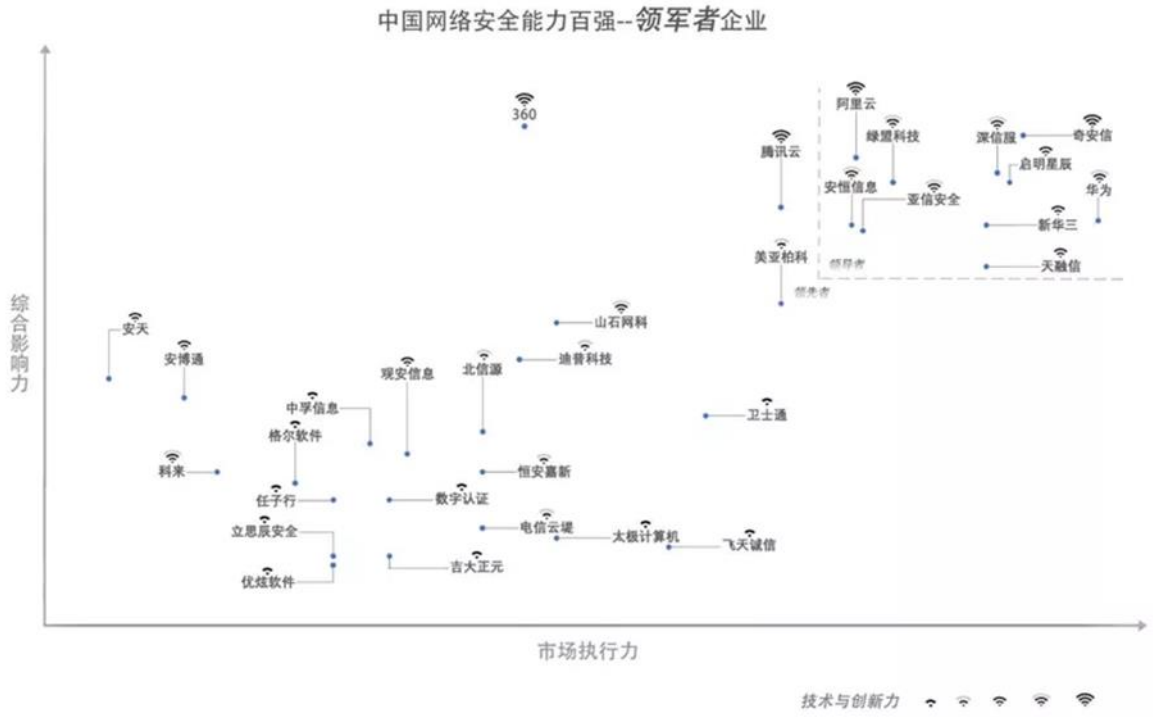


数据来源：中国网络安全产业联盟，东吴证券研究所

3. 数据驱动安全，新赛道产品竞争力强

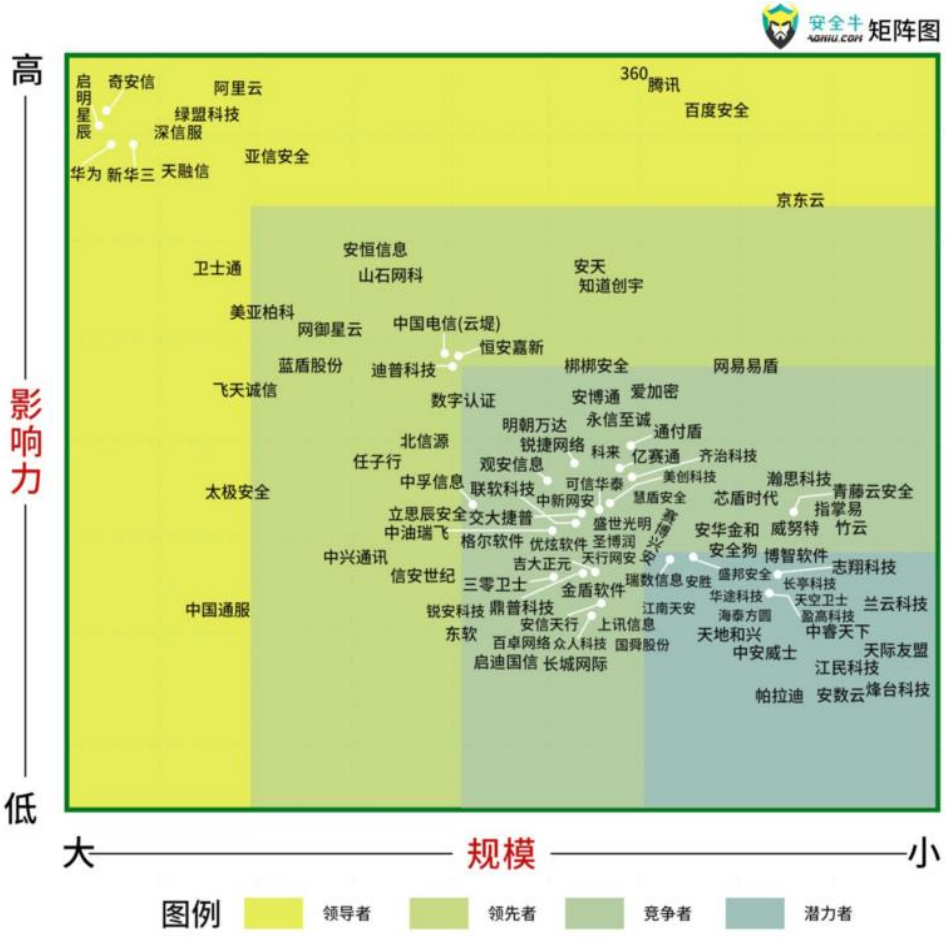
国内网络安全行业综合实力的领头羊。根据数世咨询发布《中国网络安全能力 100 强》，奇安信集团位居中国网络安全能力百强——领军者企业矩阵榜首。安全牛发布的《中国网络安全 100 强 (2019)》报告显示，网络安全企业共分为领导者、领先者、竞争者和潜力者四个梯队，奇安信集团位居领导者矩阵榜首。

图 27:《中国网络安全能力 100 强》榜首



数据来源：数世咨询，东吴证券研究所

图 28：安全牛中国网络安全百强企业榜首



数据来源：安全牛，东吴证券研究所

产品全：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，是入围该全景图细分领域最多的网络安全企业；除了传统安全产品领域（公司并购的网神和网康），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，这与如今信息技术发展中重点的发展领域相互匹配，也是网络安全市场未来发展的“主航道”。

产品强：公司核心产品和服务的技术和市场影响力获得了国内外市场研究机构的认可，主要产品和服务市场份额位居行业前列。

表 2：公司产品市场排名情况

标志性事件	来源	时间
入选全部 15 个一类、71 个二级分类安全领域，成为入围网络安全全景图细分领域最多的企业	安全牛	2020 年
Gartner 亚太区防火墙魔力象限核心厂商（2019 年）	Gartner	2019 年
中国态势感知解决方案领导者企业	IDC	2019 年

“2018 年赛迪网络安全潜力企业榜 80 强”第一名	赛迪咨询	2019 年
“云安全管理平台”、“虚拟化安全管理系统”被评为 2018-2019 中国网络信息安全市 场年度优秀产品	赛迪咨询	2019 年
“天机 TrustSpace 安全工作空间”被评为 2018-2019 中国网络信息安全市场年度创新产品奖	赛迪咨询	2019 年
2018 年度中国区 Web 安全（SaaS）市场领导者奖	FROST&SULLIVAN	2019 年
Gartner 亚太区防火墙魔力象限核心厂商（2018 年）	Gartner	2018 年
中国威胁情报安全服务市场领导者、中国态势感知解决方案领导者企业	IDC	2018 年
中国威胁情报市场领导者	安全牛	2018 年
态势感知实力矩阵规模第一	安全牛	2018 年
“态势感知项目”、“终端安全管理系统”被评为 2017-2018 中国网络信息安全市场年度最佳解决方案	赛迪咨询	2018 年
“安全服务”、“新一代智慧防火墙”被评为 2017-2018 中国网络信息安全市场年度创新产品	赛迪咨询	2018 年
2018 年度终端安全市场份额第一、安全管理平台市场份额第一、云安全市场份额第一、安全服务市场份额第一	赛迪咨询	2018 年
2018 年度终端安全软件市场份额第一	IDC	2018 年
2018 年 Web 安全市场份额第二、UTM 市场份额第二	赛迪咨询	2018 年
2018 年安全内容管理硬件市场份额第二	IDC	2018 年
2017 年入围 Gartner 终端防护平台魔力象限	Gartner	2017 年
2017 年度终端安全市场份额第二、安全管理市场份额第二、安全服务市场份额第二、Web 安全市场份额第二、UTM 市场份额第二	赛迪咨询	2017 年
2017 年度终端安全市场份额第二、安全内容管理市场份额第二	IDC	2017 年

数据来源：招股说明书，东吴证券研究所

产品高复购率：2017-2019 年，公司营收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。从普遍趋势上看，发行人历年的老客户，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 3：公司营收中新老客户贡献收入情况

项目	2017 年		2018 年		2019 年	
	收入（万元）	数量	客单价（万元）	收入（万元）	数量	客单价（万元）	收入（万元）	数量	客单价（万元）

老客户	22955.48	1261	18.2	110225.13	3278	33.63	184199.48	5127	35.93
新客户	57506.81	7029	8.18	69267.97	7449	9.3	130734.00	11746	11.13
合计/平均	80462.29	8290	9.71	179493.10	10727	16.73	314933.48	16873	18.66

数据来源：招股说明书，东吴证券研究所

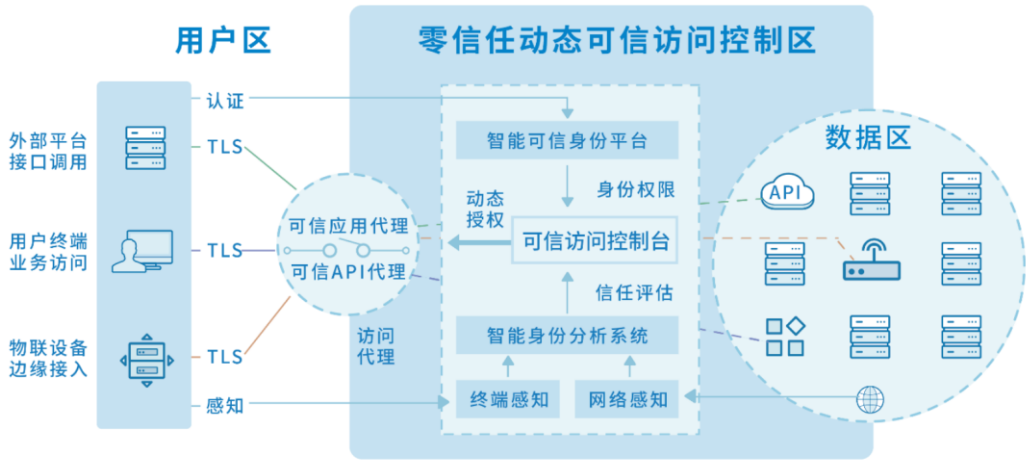
新赛道产品打造能力强。公司通过建设四大研发平台。四大研发平台聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，包括网络操作平台、大数据操作平台、可视化操作平台以及云控操作平台，将安全产品需要的通用且核心的网络流量智能解析与调度、安全大数据存储与分析、安全可视化分析与展示及云端安全管控能力平台化、模块化，使得公司的安全产品具有通用的基础架构，能够避免新产品研发过程中核心能力的重复研发，将极大降低未来新产品的研发成本及研发周期。依靠四大研发平台，当网络安全新兴领域或“新赛道”出现安全需求需要研发新产品时，公司四大研发平台可以直接提供核心安全能力，使得公司可以在较短的时间内快速发布新产品，以取得新兴领域或“新赛道”的先发优势，进一步快速抢占市场份额

3.1. 基础架构安全体系：国内领先的零信任架构践行者和标准制定者

基础架构安全类产品，围绕身份、行为和应用构建防御体系，包括以身份为中心进行动态细粒度访问控制的零信任身份安全产品、日志与审计安全产品以及应用开发安全产品。

拥有国内领先的“零信任身份安全架构”研究实验室。奇安信身份安全实验室致力于解决国内“企业物理边界正在瓦解、传统边界防护措施正在失效”的新一代网络安全问题，并推出“以身份为基石、业务安全访问、持续信任评估、动态访问控制”为核心的奇安信零信任身份安全解决方案。该团队结合行业现状，大力投入对零信任安全架构的研究和产品标准化，积极推动“零信任身份安全架构”在业界的落地实践，其方案已经在部委、央企、金融等行业进行广泛落地实施。

图 29：零信任产品架构图



数据来源：公司官网，东吴证券研究所

奇安信零信任安全解决方案主要包括：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，如下图所示。奇安信零信任安全解决方案中，动态可信访问控制平台和智能可信身份平台逻辑上进行解耦，当客户现有身份安全基础设施满足零信任架构要求的情况下，可以不用部署智能可信身份平台，通过利用现有系统可降低建设成本。

图 30：奇安信零信任安全解决方案



数据来源：公司官网，东吴证券研究所

公司牵头的零信任标准获立项。近日，全国信息安全标准化技术委员会发布了《关于 2020 年网络安全标准项目立项的通知》，由公司子公司网神股份等发起的国家标准《信息安全技术 · 零信任参考体系架构》已正式获得立项。该标准将成为继美国国家标准技术研究院(NIST)零信任架构标准后，全球第二个国家层面的零信任标准，有望填补

国内零信任领域的空白。

图 31：子公司网神等制定的零信任标准获得立项

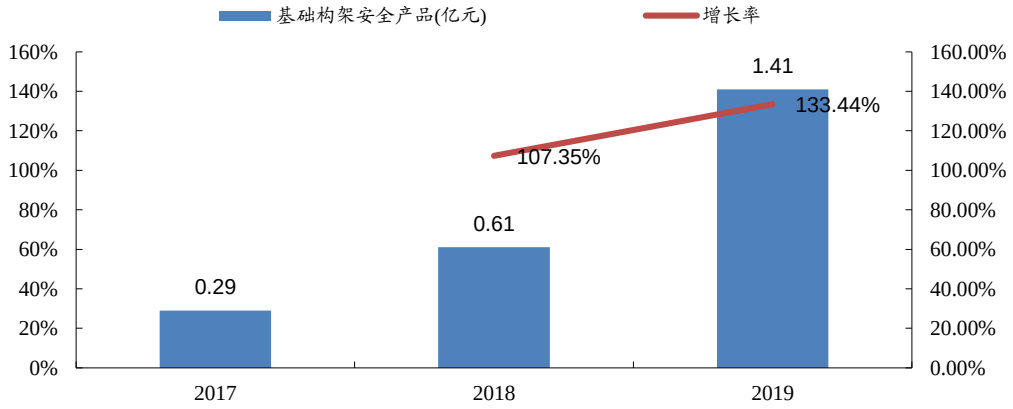
2020 年网络安全国家标准项目立项清单

序号	项目名称	工作组	标准类型	申请单位
标准制定项目（28 项）				
1.	信息安全技术 信息系统密码应用设计技术要求	WG3	制定	鼎铉商用密码测评技术（深圳）有限公司、中国科学院数据与通信保护研究教育中心、兴唐通信科技有限公司等
2.	信息安全技术 信息系统密码应用测评要求	WG3	制定	国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、公安部第三研究所等
3.	信息安全技术 人脸识别数据安全要求	WG4	制定	北京赛西科技发展有限责任公司、浙江蚂蚁小微金融服务集团股份有限公司、北京旷视科技有限公司等
4.	信息安全技术 基因识别数据安全要求	WG4	制定	深圳华大基因科技有限公司、山西医科大学、西安交通大学等
5.	信息安全技术 步态识别数据安全要求	WG4	制定	银河水滴科技（北京）有限公司、中国科学院自动化研究所、哈尔滨工程大学等
6.	信息安全技术 声纹识别数据安全要求	WG4	制定	北京得意音通技术有限责任公司、清华大学、公安部第三研究所等
7.	信息安全技术 零信任参考体系架构	WG4	制定	网神信息技术（北京）股份有限公司、中国科学院大学、中国信息通信研究院等

数据来源：公司官网，东吴证券研究所

基础架构安全产品复合增速超一倍。2017-2019 年，基础架构安全产品销售收入分别为 0.29、0.61 和 1.41 亿元，占主营业务收入的比例分别为 3.63%、3.37%和 4.49%，年均复合增长率为 120.01%。报告期内，公司基础架构安全产品收入持续增长，占主营业务收入的比重略有提升。

图 32：基础架构安全产品营收



数据来源：Wind，东吴证券研究所

基础架构安全产品销售收入的增长主要是由于“零信任基础架构”中的“零信任身

份安全”产品、“日志与审计安全”中的“日志收集与分析系统”中的“日志审计分析系统”产品、“应用开发安全”中的“代码卫士”产品的收入增长贡献，三者 2019 年营收总和为 10687.3 万元，占比约 76%。

表 4：基础架构安全产品主要收入贡献产品

		2017	2018	2019
零信任身份安全	营收(万元)			1253.55
日志审计分析系统	营收(万元)	1280.95	3551.96	5000.24
	增长率		177.29%	40.77%
代码卫士	营收(万元)	1415.59	2170.18	4532.51
	增长率		53.31%	108.85%

数据来源：招股说明书，东吴证券研究所

3.2. 新一代 IT 基础设施防护产品

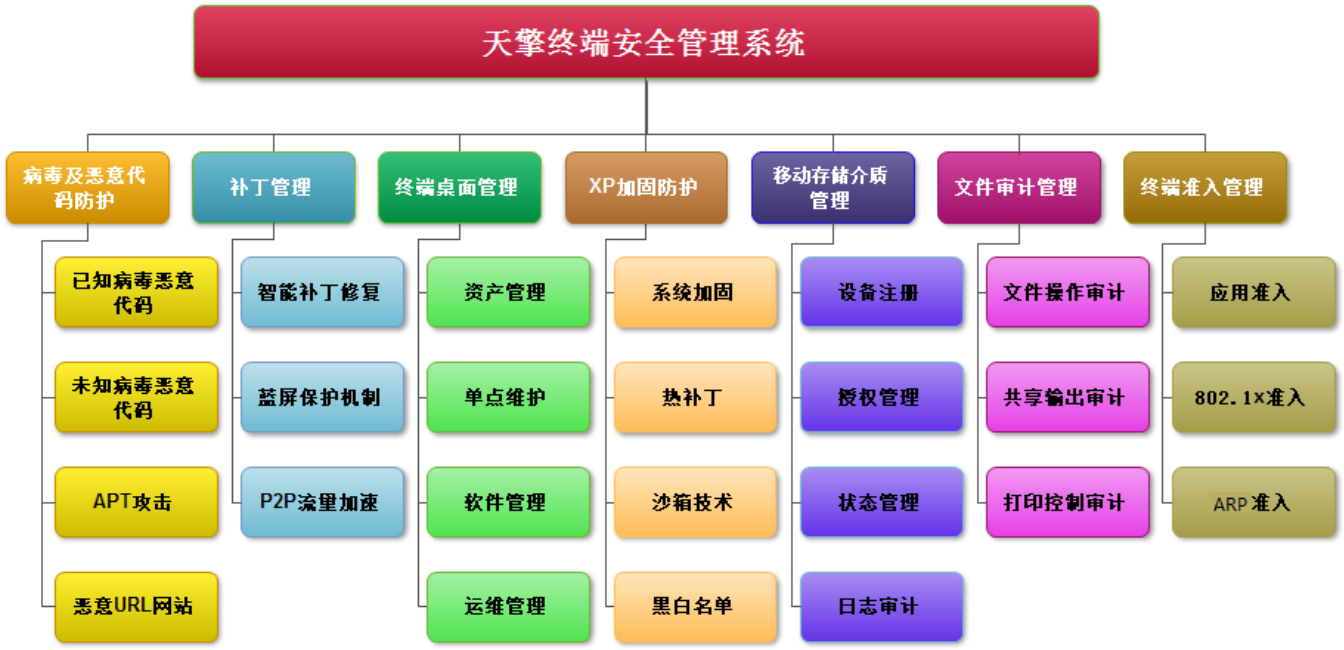
新一代 IT 基础设施防护产品，以泛终端、新边界、云计算、大数据为主要防护对象，包括泛终端安全防护、新边界安全防护、云计算基础设施安全防护、大数据基础设施安全防护等产品，确保网络安全能力覆盖新一代 IT 基础设施的万物互联接入、多类型网络传输与边界防护，基于云的混合模式计算环境，以及在各个信息化与业务系统之间的大数据流转。

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。

3.2.1. 终端安全产品：国内市场份额第一

终端安全产品天擎，该产品具有集中管理和控制、终端安全防护、漏洞和补丁管理、运维管控、移动存储管理、主机审计、检测与响应、威胁评估和终端数据安全九大功能模块，包括约 60 项细分技术功能。2019 年 7 月，发行人推出了自主研发的奇安信终端安全产品（新版天擎）。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。

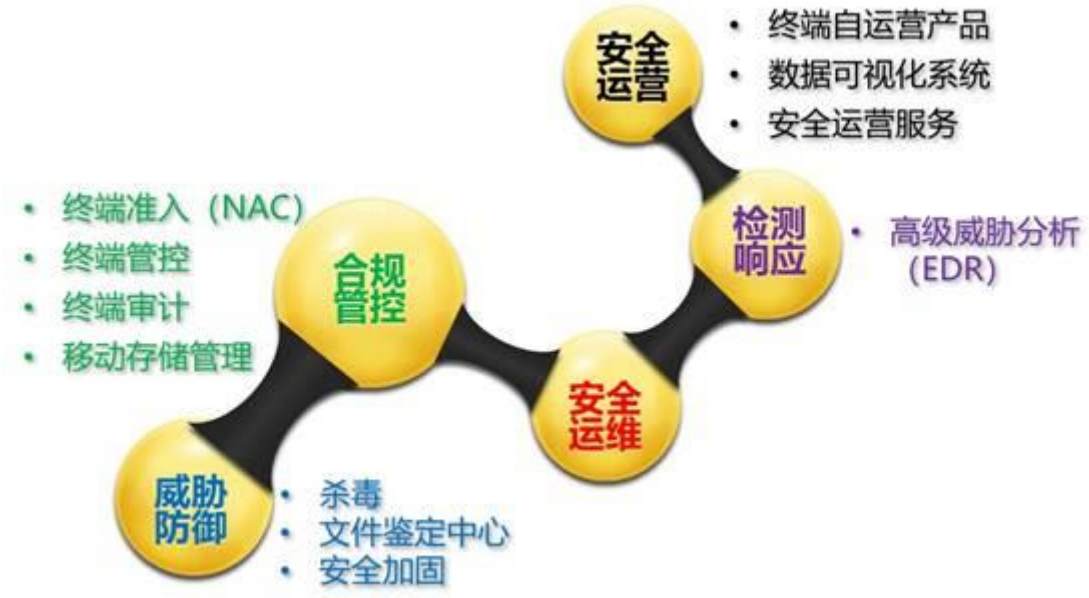
图 33：天擎终端安全管理系统功能展示



数据来源：公司官网，东吴证券研究所

奇安信终端安全管理系统，是针对政企客户在终端安全技术领域的薄弱环节，推出的一体化终端安全产品解决方案。该产品集防病毒、终端安全管控、终端准入、终端审计、外设管控、EDR 等功能于一体，兼容不同操作系统和计算平台，帮助客户实现平台一体化、功能一体化、数据一体化的终端安全立体防护。

图 34：终端安全产品结构

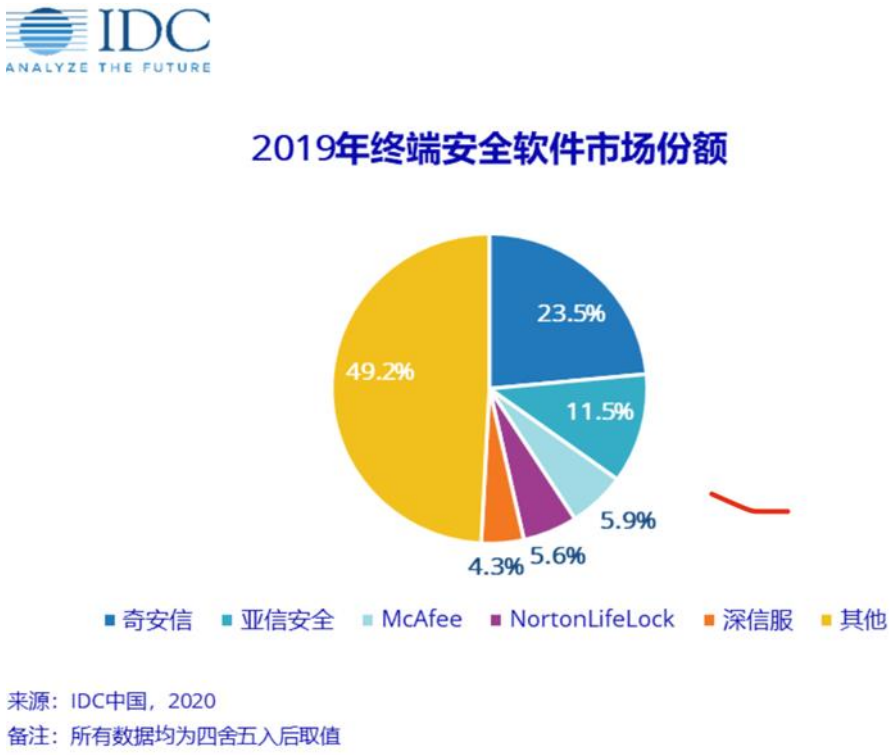


数据来源：公司官网，东吴证券研究所

国内终端安全软件市场份额排名第一。凭借领先的技术创新和运营服务能力，奇安信天擎长期处于国内终端安全市场前列。根据 IDC 发布的《2019 年下半年中国 IT 安全软件市场跟踪报告》显示，在终端安全领域，奇安信以 23.5%的市场份额，连续两年领

跑终端安全软件市场。并且伴随着中国网络安全市场的快速增长和政企客户投资向软件和服务市场的偏移，终端安全作为安全软件市场最大的子领域之一，将保持高速增长的姿态。

图 35：2019 年终端安全软件市场份额



数据来源：IDC，东吴证券研究所

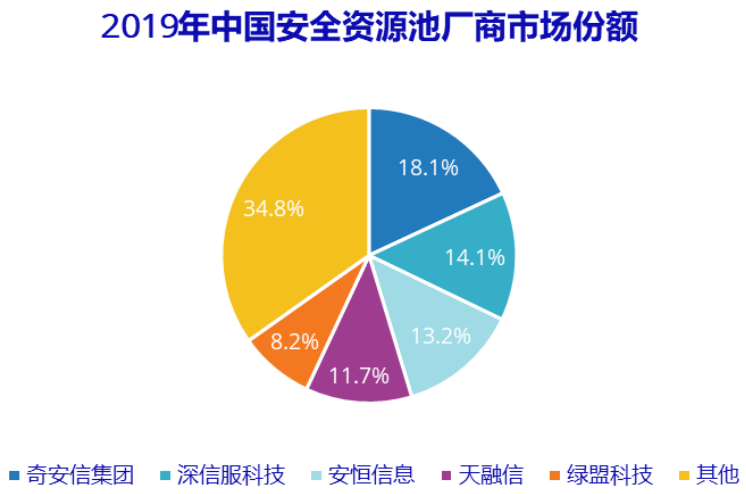
3.2.2. 私有云安全产品：国内市占率第一

应对多云环境、强化风险控制、数据安全合规等成为云安全热点领域。一是以软件定义安全为核心的云安全资源池，结合安全服务链技术，将安全服务化，用户可以根据业务的安全策略需求，自定义安全访问路径，构建自己的纵深防御体系；二是云工作负载保护平台（CWPP）功能多样化拓展，在负载分割、流量可视化、系统监控、应用管理、漏洞和配置管理等能力基础上，众多厂商积极推动云工作负载保护平台在容器安全、微隔离、态势感知、EDR 等能力拓展以及在多云环境的适配；三是容器安全，当前 PaaS 应用平台已经转向基于容器技术的平台，容器已经成为了新的虚拟化技术，此外如容器编排也是实现复杂功能的支撑技术。然而，容器自身无论在计算、存储还是网络方面，都需要事先评估其安全性。

云安全管理平台可为多种场景的用户，提供丰富的安全能力，涵盖主机、网络、应用、数据等各个层面，保障用户业务的安全。同时，用户可以利用平台提供的图形化操作形式完成安全能力编排，通过策略组合满足等级保护 2.0 的要求，并快速为用户构建纵深防御体系。

云安全管理平台国内第一。IDC 发布的《中国安全资源池市场份额，2019: 新市场、新动能、新发展》报告显示，针对中国安全资源池市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。其中，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 36：安全资源池国内市占率第一

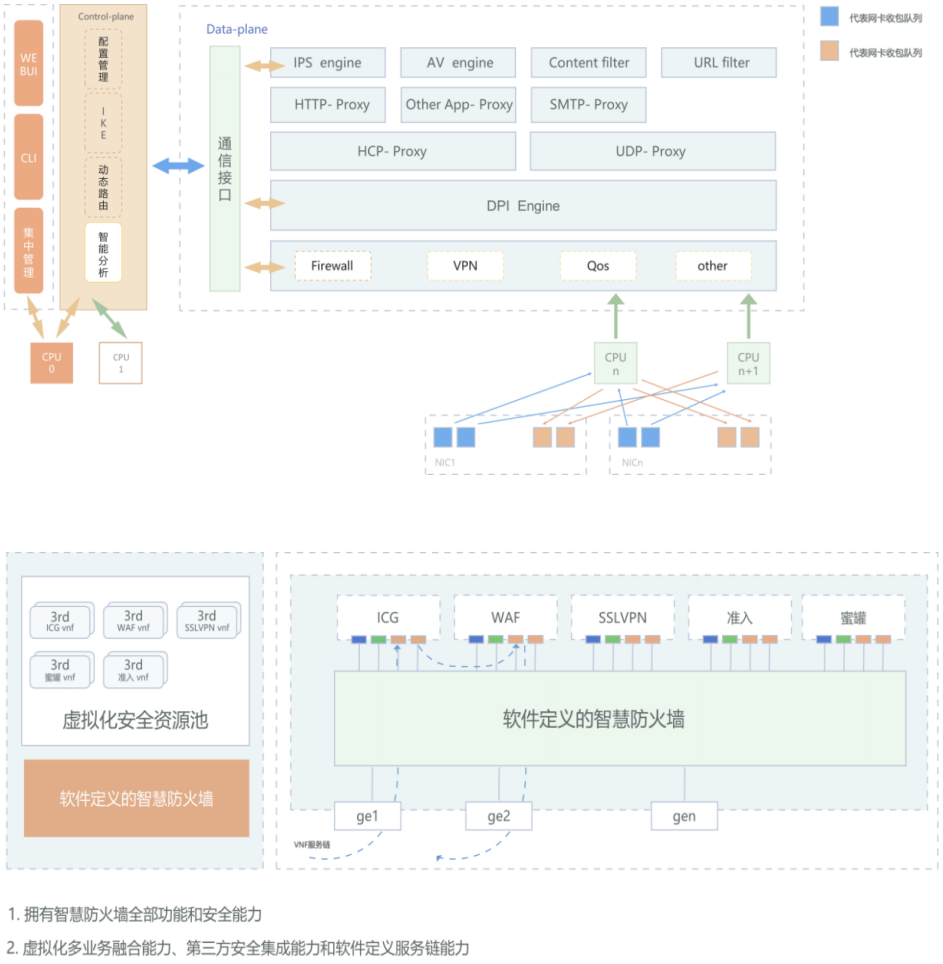


数据来源：IDC，东吴证券研究所

3.2.3. 新一代智慧防火墙入围中国移动防火墙集采项目

新一代智慧防火墙系统是公司自主创新的新一代防火墙安全系统，集成了内部多项系统的协同防御功能，同时在此基础上，由防火墙的分析中心、数据中心、处置中心实现功能一体化过程，是专门为政府、军队、金融、教育、运营商、企业的网络出口打造的基于协同防御体系的新一代安全防御系统。基于性能卓越的鲲鹏网络平台、第四代 SecOS 操作系统以及诸多数据处理机制优化，智慧防火墙可在大流量、复杂场景、多安全功能开启情况下始终保持高性能，并确保在极端条件下依然稳定可靠，能够最大程度满足运营商客户对于高性能、高可靠方面的需求。同时，借助于云端的威胁情报，智慧防火墙还可以更高效的识别并阻断突发威胁。

图 37：智慧防火墙产品架构图



1. 拥有智慧防火墙全部功能和安全能力
2. 虚拟化多业务融合能力、第三方安全集成能力和软件定义服务链能力

数据来源：招股说明书，东吴证券研究所

入围中国移动防火墙集采项目。2020 年 6 月 9 日，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**。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 38：中国移动防火墙集采中标详情，奇安信中标份额为标 3 的 20%

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%。

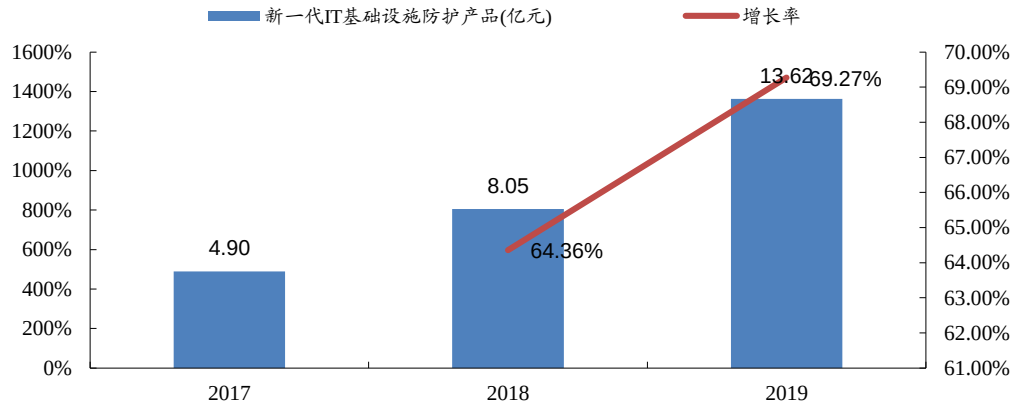
第3中标候选人：网神信息技术（北京）股份有限公司，投标报价22729980.00元（不含税），中标份额20%。

数据来源：中国移动官网，东吴证券研究所

3.2.4. 泛终端安全和云安全是主要收入增长贡献点。

新一代 IT 基础设施防护产品收入系网络安全产品销售收入的主要来源，2017 年、2018 年及 2019 年，新一代 IT 基础设施防护产品销售收入分别为 48,969.77 万元、80,488.39 万元和 136,240.67 万元，占主营业务收入的比例分别为 60.86%、44.84%和 43.26%，年均复合增长率为 66.80%。报告期内，公司新一代 IT 基础设施防护产品销售收入快速增长，是公司网络安全产品业务收入的主要组成部分。

图 39：新一代 IT 基础设施防护产品营收



数据来源：Wind，东吴证券研究所

新一代 IT 基础设施防护产品销售收入的增长主要是由于“泛终端安全防护”中的“终端安全管理系统”中的“天擎一体化终端管理系统”产品、“泛终端安全防护”中的“终端安全准入系统”产品、“新边界安全防护”中的“新一代智慧防火墙”产品、“云计算安全防护”中的“云安全管理平台”和“虚拟化安全管理系统”产品的收入增长贡献。

表 5：新一代 IT 基础设施防护产品重要产品收入

		2017	2018	2019
终端安全准入系统	营收(万元)	2013.14	4736.87	7220.67
	增长率		135.30%	52.44%
天擎一体化终端管理系统	营收(万元)	11232.34	19013.98	42182.01
	增长率		69.28%	121.85%
新一代智慧防火墙	营收(万元)	10251.87	17507.98	27627.63
	增长率		70.78%	57.80%
云安全管理平台	营收(万元)	141.85	1418.59	6723.83
	增长率		900.06%	373.98%
虚拟化安全管理系统	营收(万元)	2566.19	6036.11	8104.88
	增长率		135.22%	34.27%

数据来源：招股说明书，东吴证券研究所

3.3. 大数据智能安全检测与管控产品

大数据智能安全检测与管控产品，采用大数据技术针对威胁进行检测和响应，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与人工智能、云计算技术与 SaaS 的交付模式，为客户提供检测、感知、分析、响应等指挥和决策支撑，并协同赋能新一代 IT 基础设施防护体系。

3.3.1. 态势感知：国内市占率第一

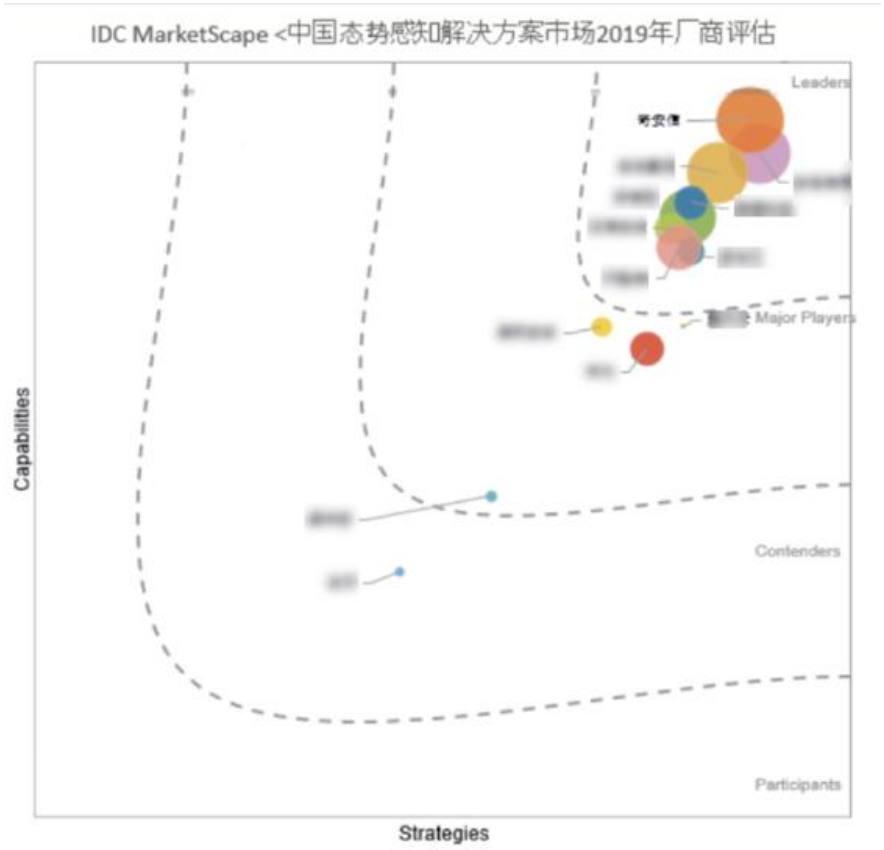
国内最大的威胁情报数据拥有者。公司拥有 IP、DNS、URL、文件黑白名单四大信誉数据库，还建立了国内名列前茅的安全威胁情报中心，也是最大的威胁情报数据拥有者之一，同时支持多种智能分析研判。公司在云端拥有海量的样本库、安全日志、DNS 解析记录和漏洞数据，在本地拥有企业全量数据的采集能力，结合机器学习和安全研究双引擎驱动，公司能够快速生产高质量的威胁情报，并实时下发到安全设备中去。

奇安信网神态势感知与安全运营平台（简称 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，已在 400+大型政企单位落地实践。

态势感知国内市占率第一。根据《IDC MarketScape:中国态势感知解决方案市场 2019 年厂商评估》报告，奇安信网络安全态势感知整体解决方案，凭借强大的产品与解决方案能力、国内第一的市场占有率，位列领导者象限。赛迪顾问发布的《2019-2020 年中国网络信息安全市场研究年度报告》和《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 连续 2 年在中国安全管理平台产品市场占有率排名第一。2020 年 3 月 19 日，数世咨询发布《网络安全态势感知能力指南》，指南显示，无论是技术创新力还是市场执行力，奇安信态势感知均位列国内第一。

图 40：奇安信在 IDC2019 年态势感知厂商评估中拍第一

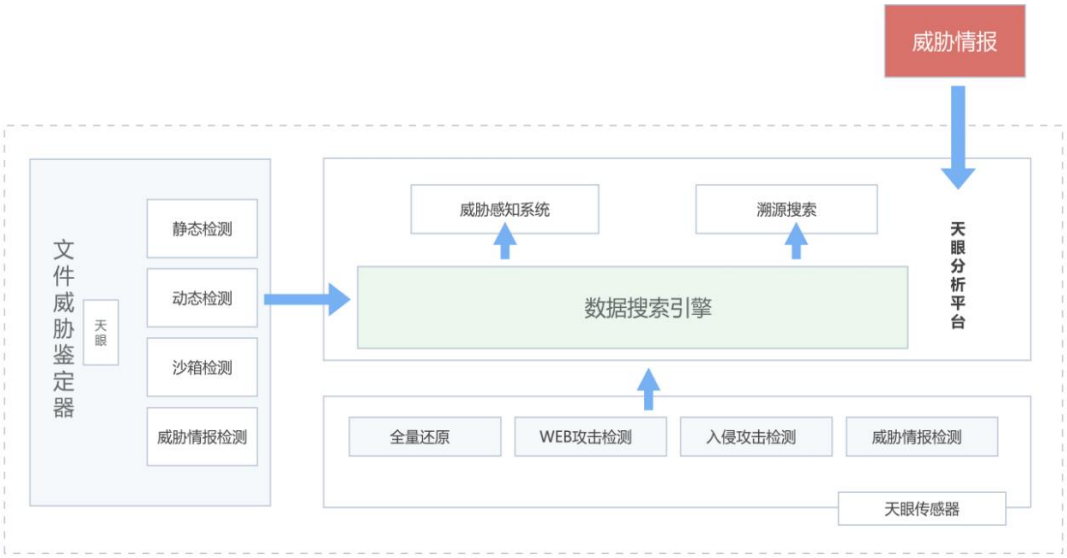


数据来源：IDC，东吴证券研究所

3.3.2. 百场实战攻防磨炼利器“天眼”

新一代威胁感知系统（SkyEye，以下简称天眼系统）以攻防渗透和数据分析为核心竞争力，聚焦威胁检测和响应，为客户提供安全服务与产品解决方案。天眼基于网络流量和终端 EDR 日志，运用威胁情报、规则引擎、文件虚拟执行、机器学习等技术，精准发现网络中针对主机与服务器的已知高级网络攻击和未知的新型网络攻击的入侵行为，利用本地大数据平台对流量日志和终端日志进行存储和查询，结合威胁情报和攻击链分析对事件进行分析、研判和回溯，同时结合边界 NDR、终端 EDR 以及自动化编排处置可以及时的阻断威胁。

图 41：新一代威胁感知与响应系统（“天眼”）产品架构图



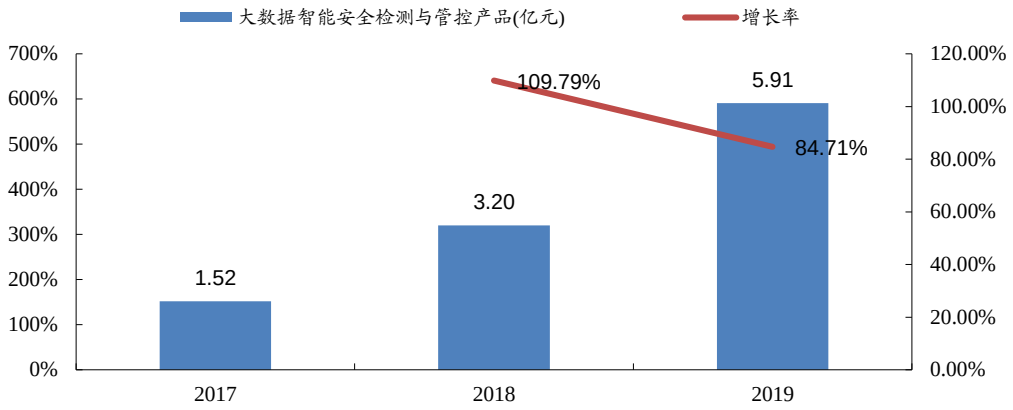
数据来源：招股说明书，东吴证券研究所

在 2019 年攻防演习过程中，天眼深入到 120 多个攻防对抗的战场，采集需求三百多条，切实的来提升天眼产品能力，并规划出实战化威胁运营平台、邮件威胁检测系统等满足实战攻防场景的产品和组件。天眼系统的客户超过 1000 家，遍及全国各省份，在公检法、金融、政府部委、运营商、石油石化、电力、教育、医疗等行业都具有成功案例，帮助客户发现和处置超过百起 APT 攻击事件。在十九大重保、一带一路、两会等重要时期以及攻防演习期间，现场的安全专家通过天眼系统累计监测攻击行为 30 余万次，发现漏洞利用行为上千起，根据攻击信息有效的协助用户对上百台服务器进行加固防护，

3.3.3. 态势感知高速增长

2017 年、2018 年及 2019 年，大数据智能安全检测与管控产品收入分别为 15,249.15 万元、31,991.56 万元和 59,091.48 万元，占主营业务收入的比例分别为 18.95%、17.82%和 18.76%，年均复合增长率为 96.85%。2019 年，公司大数据智能安全检测与管控产品销售收入占主营业务收入的比例有所提高，增速高于网络安全产品业务整体增速，是公司网络安全产品业务的重要发展方向。

图 42：大数据智能安全检测与管控产品营收



数据来源：Wind，东吴证券研究所

态势感知产品在加速增长。政企态势感知与安全运营管理平台（NGSOC）、网络空间安全态势感知与通报处置平台、新一代威胁态势感知与响应系统过去两年均保持高速的增长，是大数据智能安全检测与管控产品收入高增长的主要收入来源，2018-2019 年的合计增速为 103.45%、177.97%，整体增长在加速。

表 6：以态势感知为代表的大数据安全产品高速增长

		2017	2018	2019
政企态势感知与安全运营管理平台（NGSOC）	营收(万元)	2358.88	5403.55	14031.66
	增长率		129.07%	159.67%
网络空间安全态势感知与通报处置平台	营收(万元)	4618.33	6733.43	15015.88
	增长率		45.80%	123.00%
新一代威胁态势感知与响应系统	营收(万元)	1781.71	5682.85	20487.11
	增长率		218.95%	260.51%
合计	营收(万元)	8758.92	17819.83	49534.65
	增长率		103.45%	177.97%

数据来源：招股说明书，东吴证券研究所

4. 打造创新式全链条网络安全服务，在信创 PKS 体系中扮演重要角色

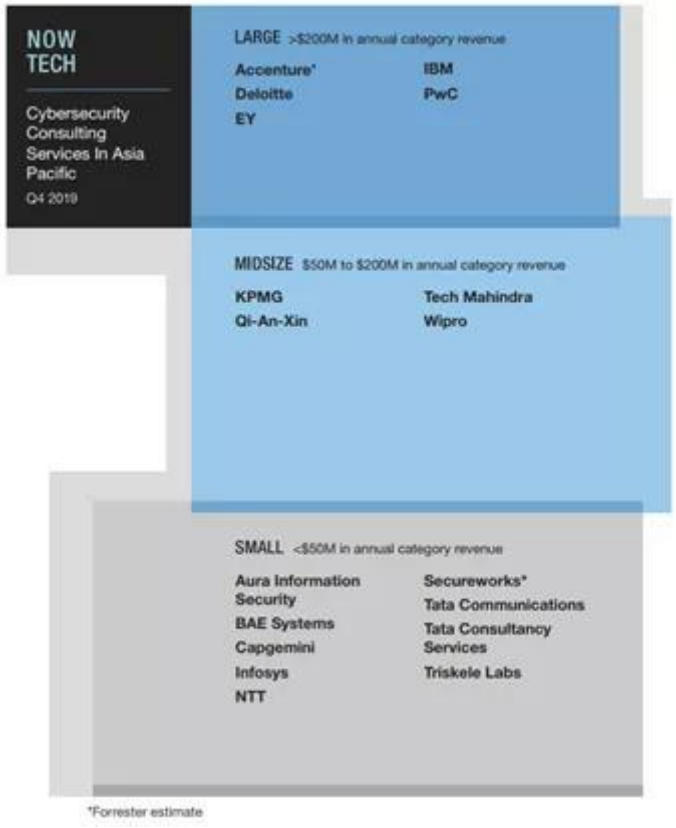
4.1. 网络安全服务：打造创新式全链条安全服务

创新的安全咨询规划服务能力。公司在创立之初，发现安全产业的最大问题就是缺少系统规划，无法满足客户中长期的信息化发展需求，进而导致安全产业规模太小。公司以“内生安全”为核心理念，与信息化过程同步规划、同步建设和同步运行，采用系

统工程的方法论，在信息化新建或改造中协助客户开展安全规划工作，确保安全和信息化真正形成了“一体化之两翼”、“双轮驱动”的效果。在十三五期间和即将开始的十四五阶段，公司帮助众多大中型客户有效开展安全咨询和规划，提升了网络安全在信息化投资中的预算占比，真正实现了网络安全保障信息化投资。

安全咨询领跑国内安全公司。全球权威市场研究与咨询机构 Forrester 正式发布《Now Tech: Cybersecurity consulting Services In Asia Pacific, Q4 2019》报告。奇安信凭借全面的安全咨询和服务能力，与毕马威等传统安全咨询巨头同时入围中型厂商阵营，作为亚太地区唯一入围中国安全公司，奇安信强势领跑国内网络安全咨询和服务市场。

图 43：领跑国内安全资讯市场



数据来源：Forrester，东吴证券研究所

庞大的安服团队和覆盖全国的应急响应中心。公司建立了覆盖全国 31 个省市自治区的应急响应中心，技术支持及安全服务人员的人数超过 2500 人，向客户（包含已有客户和潜在客户）提供应急响应技术服务。2019 年，公司共参与和处置了 2,000 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 1,000 人支撑新中国 70 周年国庆网络安保等。

超强的实战攻防服务能力。奇安信在成立之初就更强调实战化的网络攻防能力而不局限于网安合规建设能力。在近年国家级的年度网络攻防演习中，公司成绩均名列前茅，

在累计几百家参加演习的单位中，超过半数单位聘请公司作为主力防护队伍；在各省、部级部门组织的网络攻防演习中，由公司承办、参与的超过三分之二以上比例，得到了头部客户的广泛认可。在漏洞报告和响应方面，公司建立的“补天漏洞平台”是 2017-2019 年对 CNVD 漏洞共享平台贡献最多的中文漏洞响应平台，三年来累计为 CNVD 报送漏洞超过十万个，补天漏洞响应平台已成为重要机构和企事业单位漏洞响应的重要保障力量。超强的实战攻防服务能力在政企攻防演习中为公司赢得口碑，带动公司产品高速增长。

创新的安全运营模式。依托大数据和云计算的技术和数据优势，公司提出以“人+工具+数据+平台”的模式，不断强化以安全运营平台和安全大数据能力及多款标准化安服工具对人进行赋能，中长期降低安全服务对人的依赖，提供了以威胁情报为代表的数据订阅和基于云计算的安全运营等创新型的云化产品，以及基于远程平台支持安全运营服务、基于城市/行业安全运营中心的“管家式”安全服务。

表 7：安全运营提供的多类型服务

类别	主要内容
以威胁情报为代表的数据订阅云化产品	通过对安全大数据的实时或离线的分析和运营，公司形成了精准、丰富的威胁情报数据，这些数据可以帮助客户持续、快速和高效的检测新兴安全威胁，客户只需要订阅数据订阅服务，公司即刻把威胁情报数据实时推送到客户的安全设备或系统，有效提升了其防护能力。
基于云计算模式的安全运营云化产品	公司将核心产品的安全能力实现了云化部署，形成了云端的安全清洗中心，客户仅仅需要开通一个服务账号，就可以将其网络或终端防护托管给云端安全清洗中心。通过这种模式，公司实现了多租户的云安全服务，这些服务完全在云端实时、按需开通，交付和维护不需要到用户现场。
基于远程平台支持安全运营服务	为了满足大型客户网络安全防护的需求，公司集中了一批能够与顶级黑客和 APT 组织进行攻防对抗的专家，远程支持现场攻防技术工程师，为重要客户提供以结果为导向的高级网络安全服务，现场专家处置一般性的网络攻击事件，而把疑难的高级攻击事件交由远程专家指导，以便及时有效处置。
基于城市/行业安全运营中心的“管家式”安全服务	鉴于安全是动态的，新的攻击方法的出现时常导致现有的安全系统失灵。因此，客户希望雇请安全公司提供“物业式”网络安全防护服务，以满足其网络安全需求；这样客户就不用过度关注购买什么设备、采用什么技术，而是通过支付服务费、设置服务标准、检查服务结果来解决网络安全问题。为此，公司设计了城市/行业安全运营中心模式，为支付服务费的客户提供优质的网络安全防护服务，包括在客户现场安装必要的设备和派出必要的人员。

数据来源：招股说明书，东吴证券研究所

打造安全人才虎符基地。虎符基地是承载奇安信集团“以人为核心的安全运营服务”

战略的重要主体，已经在绵阳和青岛建立安全运营人才的培训基地，致力于网络空间安全专业人才的培养和面向全国提供安全运营服务，解决行业对大量网络信息安全人才的需求，持续提升为党政军以及广大企事业单位网络安全保驾护航的服务能力和水平。2019 年与中国工程物理研究院培训中心签署了联合建设军工行业网络安全人才培养基地协议，持续拓宽服务领域，探索新的培养模式。截至 2019 年 12 月份奇安信虎符基地共举办 22 期网络安全特训班，培养网络安全人才超过 1500 人，为集团选拔输送了近千名网络安全运营服务工程师，这些工程师服务于政府、教育、金融、能源等各条业务线，遍布全国 60 多个城市。

图 44：人才培养基地布局图



数据来源：公司官网，东吴证券研究所

2019 年新安全服务企业 top1。《互联网周刊》和 eNet 研究院联合发布了"2019 年度新安全服务企业 TOP50"，奇安信凭借在大数据与安全智能、终端安全防护、安全运营与应急响应等领域的综合实力，荣膺榜首。这也是继 2019 年 10 月份奇安信获得"2019 企业网络安全服务 TOP10"榜单第一名之后，再次斩获殊荣。

图 45：2019 年信安全服务企业排名第一

2019 年度新安全服务企业 TOP50

排名	企业	备注
1	奇安信	大数据与安全智能、终端安全防护等
2	安恒信息	应用安全、大数据安全、云安全、物联网安全等
3	亚信安全	云安全、终端安全、态势感知、高级威胁治理等
4	蓝盾股份	安全产品、安全服务、安全运营
5	卫士通	密码产品、网络安全、安全运维等
6	青藤云	以服务器安全为核心的云安全
7	美亚柏科	互联网舆情监测与预防、网络安全防护
8	华为	云安全、通信安全
9	东软网络安全	安全应用、安全产品、安全解决方案
10	山石网科	边界安全、云安全、数据安全、内网安全
11	恒安嘉新	通信网安全、网络空间安全基础与生态搭建
12	腾讯安全	互联网安全（终端安全、数据安全、云安全等）
13	迪普科技	网络安全、应用安全、云安全
14	百度安全	AI 安全、数据安全、云安全等

数据来源：《互联网周刊》和 eNet 研究院，东吴证券研究所

4.2. 拥抱信创，有望在中国电子 PKS 体系中扮演重要角色

多款产品已适配国产软硬件平台。金融、运营商等行业的安全市场领域，仍拥有一定海外安全厂商的身影。随着信创领域的开展，国产厂商正积极投入国产体系建设，进一步实现对国外品牌的替代。奇安信网神终端安全管理系统等奇安信集团旗下多款产品，已逐步实现对飞腾、龙芯、兆芯、申威、海光、鲲鹏等 CPU 以及麒麟软件、中科方德、UOS 等主流信创平台的全面兼容适配，该安全管理系统及一体化防护解决方案已在客户侧投入稳定运行，为信创生态网络安全保驾护航。

图 46：奇安信网神终端安全管理系统在麒麟 v10 上运行状况

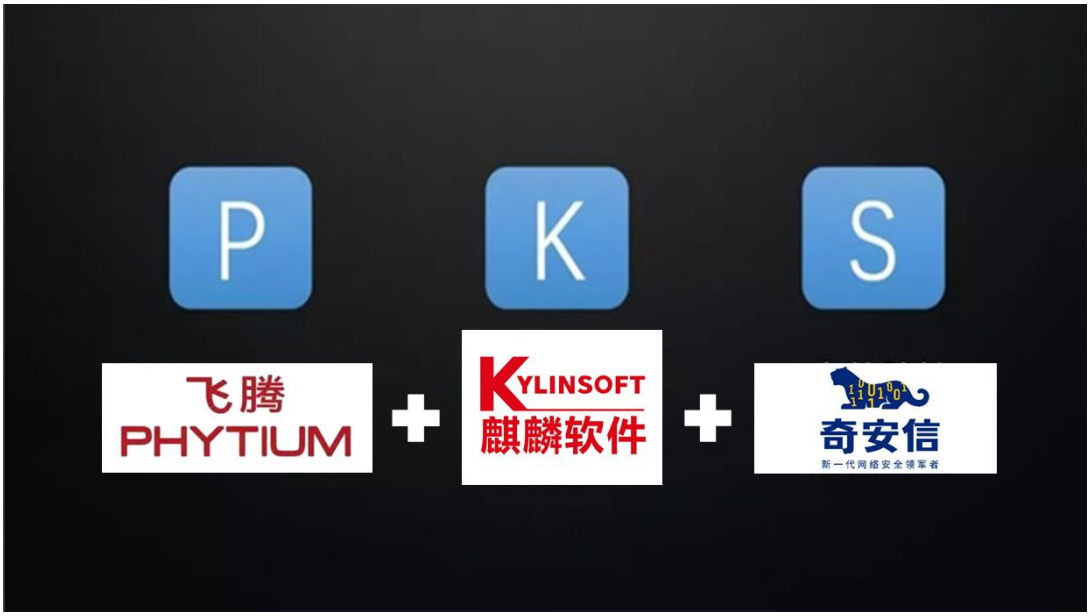
请务必阅读正文之后的免责声明部分



数据来源：公司官网，东吴证券研究所

从“PK”体系到“PKS”体系，奇安信有望在“S”中占据重要地位。2018 年，中国电子在原有“PK”体系的基础架构中，加入“S-Security”立体防护的安全链，推出了“PKS”安全体系，主要解决计算机体系结构缺乏免疫力、产品应用补修漏洞不及时、常规安全防护机制降低 CPU 功效的问题。“PKS”体系中“S”的安全能力主要体现在两方面：“可信计算”和“网络安全”。PKS(飞腾 CPU+麒麟操作系统+网络安全)体系生态——通过“关后门、防漏洞、防断供”，打造并实践了本质安全、过程安全、产业安全三大战略。2019 年 5 月中国电子以 37 亿元战略入股奇安信，这意味着奇安信将安全技术与安全人才双向加持中国电子网络安全能力，双方深度融合，奇安信有望在“S”中占据重要地位。

图 47：在新的 PKS 体系中，奇安信有望在 S 环节占据重要地位



数据来源：各公司官网，东吴证券研究所整理

5. 盈利预测与估值

IDC 预测 2020-2024 年中国安全市场 CAGR 为 18.7%，其中硬件市场、软件市场、服务市场 CAGR 分别为 18.5%、30%、21.0%。

1）网络安全产品：预计 2020 年-2022 年营收增速为 44.40%、44.39%、40.89%；其中：

①新一代 IT 基础设施防护产品：云安全和泛终端安全需求相对稳步增长，预计 2020 年-2022 年增速为 39%、40%、35%；

②大数据智能安全监测与管控产品： 2017-2019 年重要产品收入复合增速较高，NGSOC 等态势感知产品处于需求仍处于爆发阶段，预计 2020 年-2022 年大数据智能安全监测与管控产品增速为 50.00%、50.00%、50.00%；

③基础架构安全产品：以零信任身份安全、日志收集与分析系统、代码卫士等产品为代表的产品尤其是零信任产品，需求处于刚爆发阶段，快速增长的趋势仍有望保持，预计 2020 年-2022 年 73%、58%、50%；

2）网络安全服务：网络安全盈利模式由软硬件产品向服务转型，安全服务市场增速将高于行业整体增速。公司安全服务业务近几年保持高速增长，预计未来几年将保持高速增长态势，预计 2020 年-2022 年网络信息安全服务增速为 50%、50%、48%；

3）硬件及其他：公司未来会逐步低毛利率的硬件业务的投入，预计 2020-2022 年网络信息安全平台业务增速为 31%、25%、20%。

图 48：营收拆分与预测（单位：百万元）

	2017	2018	2019	2020E	2021E	2022E
网络安全产品	671.37	1185.32	2094.59	3024.51	4366.94	6152.73
增速		76.55%	76.71%	44.40%	44.39%	40.89%
占比	81.75%	65.24%	66.41%	67.50%	69.05%	70.46%
营业成本	150.31	326.19	563.40	768.04	1084.61	1494.74
营业成本率	22.39%	27.52%	26.90%	25.39%	24.84%	24.29%
毛利率	77.61%	72.48%	73.10%	74.61%	75.16%	75.71%
新一代 IT 基础设施防护产品	489.70	804.88	1362.41	1893.75	2651.25	3579.19
增速		64.36%	69.27%	39.00%	40.00%	35.00%
占比	59.63%	44.30%	43.19%	42.26%	41.92%	40.99%
营业成本	114.58	240.18	357.89	492.37	676.07	894.80
营业成本率	23.40%	29.84%	26.27%	26.00%	25.50%	25.00%
毛利率	76.60%	70.16%	73.73%	74.00%	74.50%	75.00%
大数据智能安全监测与管控产品	152.49	319.92	590.91	886.37	1329.55	1994.32
增速		109.79%	84.71%	50.00%	50.00%	50.00%

占比	18.57%	17.61%	18.73%	19.78%	21.02%	22.84%
营业成本	31.61	74.61	179.10	230.45	339.03	498.58
营业成本率	20.73%	23.32%	30.31%	26.00%	25.50%	25.00%
毛利率	79.27%	76.68%	69.69%	74.00%	74.50%	75.00%
IT 基础架构、工具及安全类产品	29.19	60.52	141.27	244.40	386.15	579.22
增速		107.35%	133.44%	73.00%	58.00%	50.00%
占比	3.55%	3.33%	4.48%	5.45%	6.11%	6.63%
营业成本	4.12	11.40	26.42	45.21	69.51	101.36
营业成本率	14.11%	18.84%	18.70%	18.50%	18.00%	17.50%
毛利率	85.88%	81.17%	81.30%	81.50%	82.00%	82.50%
网络安全服务	111.77	219.75	367.32	550.98	826.47	1223.18
增速		96.62%	67.15%	50.00%	50.00%	48.00%
占比	13.61%	12.10%	11.65%	12.30%	13.07%	14.01%
营业成本	35.33	94.37	135.02	203.86	309.93	464.81
营业成本率	31.61%	42.94%	36.76%	37.00%	37.50%	38.00%
毛利率	68.39%	57.06%	63.24%	64.00%	64.50%	65.00%
硬件及其他	21.48	389.86	687.42	900.52	1125.65	1350.78
增速		1714.71%	76.32%	31.0%	25.0%	20.0%
占比	2.62%	21.46%	21.79%	20.10%	17.80%	15.47%
营业成本	20.43	384.55	665.59	873.51	1091.88	1310.26
营业成本率	95.08%	98.64%	96.82%	97.00%	97.00%	97.00%
毛利率	4.92%	1.36%	3.18%	3.00%	3.00%	3.00%
其他业务	16.62	21.84	4.79	5.03	5.28	5.55
增速		31.41%	-78.05%	5.00%	5.00%	5.00%
占比	2.02%	1.20%	0.15%	0.11%	0.08%	0.06%
营业成本	0.01	0.00	0.97	1.01	1.06	1.11
营业成本率	0.06%	0.00%	20.25%	20.00%	20.00%	20.00%
毛利率	99.97%	100.00%	79.72%	80.00%	80.00%	80.00%
收入总计	**821.24**	**1816.77**	**3154.12**	**4481.05**	**6324.35**	**8732.24**
增速		121.22%	73.61%	42.07%	41.14%	38.07%
成本总计	**206.08**	**805.10**	**1364.97**	**1846.42**	**2487.48**	**3270.92**
增速		290.68%	69.54%	35.27%	34.72%	31.50%
毛利率	**74.91%**	**55.68%**	**56.72%**	**58.79%**	**60.67%**	**62.54%**

数据来源：Wind，东吴证券研究所

盈利预测与投资建议：预计公司 2020-2022 年营收分别为 44.81 亿元、63.24 亿元、87.32 亿元，增速分别为 42.07%、41.14%、38.07%，归母净利润分别为-2.12 亿元、1.29 亿元、5.51 亿元，增速分别为 57.1%、160.6%、328.1%。

作为国内网络安全领域的龙头和国家队，应对新的网络安全需求背景，积极打造面向万物互联时代的网络安全协同联动防御体系，重点布局新赛道产品和庞大的安全服务团队建设，目前仍处于相对高投入和前期布局阶段，投入较大费用，仍处于亏损阶段，因此考虑采取 PS 估值。

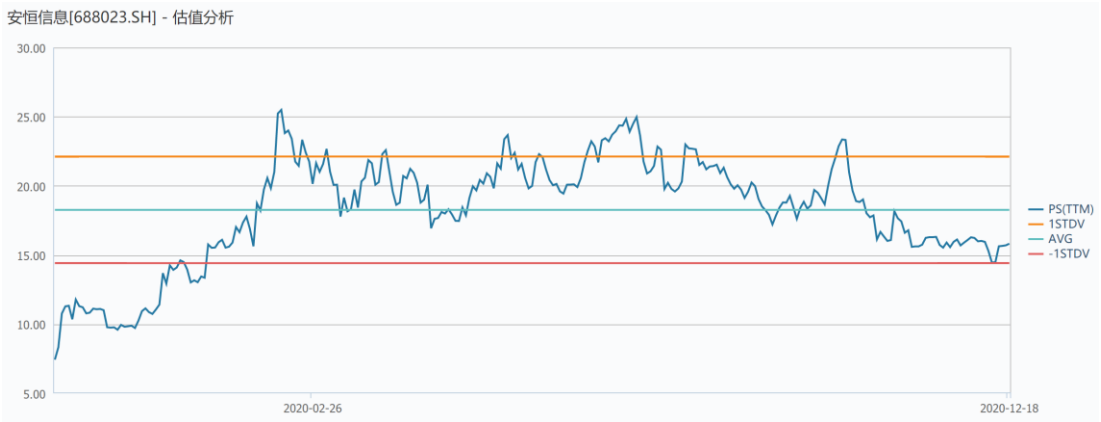
PS 估值：以行业相关性、产品结构相似性为标准，国内公司选取安恒信息、深信服、山石网科、安博通等网安公司作为可比标的，国外公司选取 Palo Alto、Crowdstrike 和 Okta 作为可比标的。目前国内新兴网络安全公司的合理 PS 估值大约为 15 倍左右，而营收高增速的安恒享受一定 PS 溢价，上市以来 PS（TTM）平均值为 18 倍，最高为 25 倍。对比国外公司，Palo Alto、Crowdstrike 和 Okta 在处于营收高增速的时期，PS 均表现的更好，即高营收增速享受高 PS，Palo Alto 高增长阶段 PS 最高达 19 倍，Crowdstrike 则一直处于高 PS 阶段，平均 PS 接近 40 倍，Okta 自 2016 年以来营收增速一直保持在 40%以上，平均 PS（TTM）高达 26 倍。目前奇安信仍处于高速增长的趋势中，考虑公司在新兴安全领域的竞争优势、行业地位（绝对龙头）以及高成长速度，可以享受一定估值溢价，而给予公司 2021 年产品和服务 18 倍 PS，对应目标市值约为 934.82 亿元，对应目标价 137.47 元，首次覆盖给予“买入” 评级。

表 8：行业可比标的估值（截至 10 月 11 日）

	公司	营收 2019（亿元）	营收 2020E（亿元）	营收 2021E（亿元）	市值（亿元）	2019PS	2020PS	2021PS	评级
688023.SH	安恒信息	9.44	13.72	20.11	179.27	19	13	9	买入
300454.SZ	深信服*	45.90	58.60	79.83	900.05	20	15	11	未评级
688030.SH	山石网科*	6.75	8.03	10.06	56.95	8	7	6	未评级
688168.SH	安博通*	2.49	3.29	4.42	31.03	12	9	7	未评级
					平均值	15	11	8	
					中位数	16	11	8	

数据来源：Wind，东吴证券研究所（带*公司盈利预测取自 Wind 一致预期）

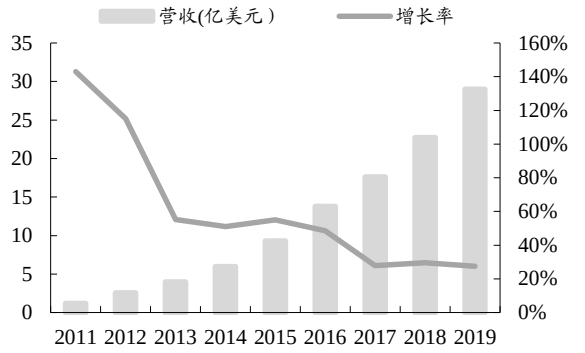
图 49：安恒信息上市以来 PS（TTM）（截止 2020.12.20）



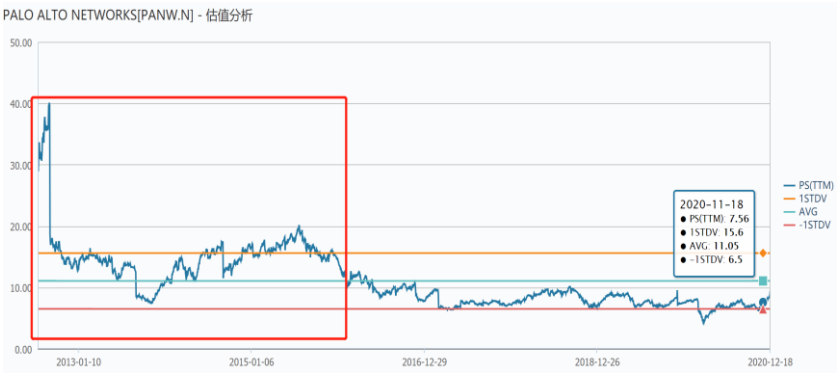
数据来源：Wind，东吴证券研究所

图 50：Palo Alto 过去 9 年营收和增速

图 51：Palo Alto 过去 9 年 PS（TTM）（截止 2020.12.20）

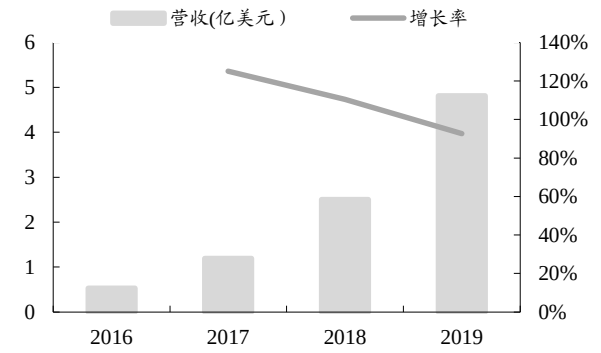


数据来源：Wind，东吴证券研究所



数据来源：Wind，东吴证券研究所

图 52：Crowdstrike 过去 4 年营收和增速



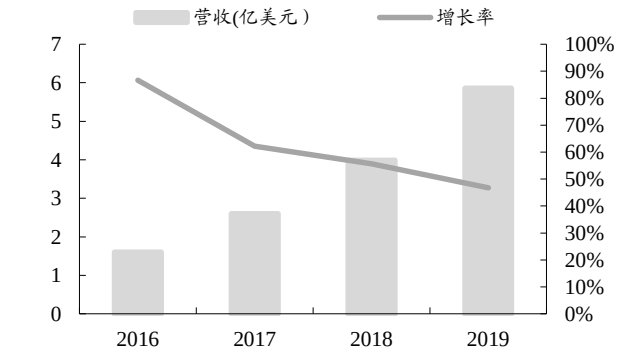
数据来源：Wind，东吴证券研究所

图 53：Crowdstrike 上市以来 PS（TTM）（截止 2020.12.20）



数据来源：Wind，东吴证券研究所

图 54：Okta 过去 4 年营收和增速



数据来源：Wind，东吴证券研究所

图 55：Okta 上市以来 PS（TTM）（截止 2020.12.20）



数据来源：Wind，东吴证券研究所

6. 风险提示

1、 **网络安全行业推进不及预期：**网安行业目前受政策、新技术、新体系、模式转型等多重利好下处于高速增长态势，若当中一两个因素推进不及预期使得整个行业客户需求不及预期，从而影响公司的发展速度。

2、 **商誉减值风险：**截止 2019 年末，公司上虞的账面价值为 12.09 亿元，主要是控股合并网神股份、网康科技等企业所致，未来市场环境发生重大不利变化等因素导致业务开展未达到预期，从而导致并购企业存在商誉减值的风险。

奇安信三大财务预测表

资产负债表（百万元）	2019A	2020E	2021E	2022E
流动资产	**3,989**	**9,466**	**9,720**	**10,200**
现金	1,258	6,253	5,181	4,679
应收账款	1,297	1,317	2,373	2,722
存货	749	1,090	1,388	1,871
其他流动资产	684	806	778	929
非流动资产	**3,166**	**3,579**	**4,075**	**4,840**
长期股权投资	392	332	273	214
固定资产	195	448	721	1,121
在建工程	995	1,212	1,491	1,910
无形资产	66	70	76	83
其他非流动资产	1,518	1,517	1,514	1,512
资产总计	**7,155**	**13,045**	**13,796**	**15,040**
流动负债	**1,968**	**2,375**	**2,983**	**3,615**
短期借款	0	0	0	0
应付账款	862	1,039	1,522	1,846
其他流动负债	1,107	1,336	1,461	1,769
非流动负债	**146**	**146**	**146**	**146**
长期借款	0	0	0	0
其他非流动负债	146	146	146	146
负债合计	**2,114**	**2,521**	**3,129**	**3,761**
少数股东权益	18	-5	9	70
归属母公司股东权益	5,022	10,529	10,658	11,209
负债和股东权益	**7,155**	**13,045**	**13,796**	**15,040**

现金流量表（百万元）	2019A	2020E	2021E	2022E
经营活动现金流	-1,114	-587	-979	-167
投资活动现金流	-219	-249	-328	-571
筹资活动现金流	927	5,832	235	235
现金净增加额	-406	4,995	-1,072	-502
折旧和摊销	140	79	134	209
资本开支	283	472	556	824
营运资本变动	-609	-75	-718	-350

利润表（百万元）	2019A	2020E	2021E	2022E
营业收入	**3,154**	**4,481**	**6,324**	**8,732**
减:营业成本	1,365	1,846	2,487	3,271
营业税金及附加	33	47	66	91
营业费用	1,118	1,389	1,771	2,358
管理费用	470	1,792	2,403	3,056
财务费用	22	-113	-235	-235
资产减值损失	-3	-5	-7	-9
加:投资净收益	196	243	303	403
其他收益	0	0	0	0
营业利润	**-536**	**-233**	**141**	**604**
加:营业外净收支	-3	-0	-1	-1
利润总额	**-539**	**-233**	**141**	**603**
减:所得税费用	14	2	-2	-9
少数股东损益	-58	-23	14	61
归属母公司净利润	**-495**	**-212**	**129**	**551**
EBIT	-576	-346	-31	455
EBITDA	-436	-267	103	664

重要财务与估值指标	2019A	2020E	2021E	2022E
每股收益(元)	-0.73	-0.31	0.19	0.81
每股净资产(元)	7.39	15.49	15.68	16.49
发行在外股份(百万股)	578	680	680	680
ROIC(%)	-11.6%	-3.3%	-0.3%	4.1%
ROE(%)	-11.0%	-2.2%	1.3%	5.4%
毛利率(%)	56.7%	58.8%	60.7%	62.5%
销售净利率(%)	-15.7%	-4.7%	2.0%	6.3%
资产负债率(%)	29.5%	19.3%	22.7%	25.0%
收入增长率(%)	73.6%	42.1%	41.1%	38.1%
净利润增长率(%)	43.2%	57.1%	160.6%	328.1%
P/E	-161.89	-377.32	622.51	145.40
P/B	15.95	7.61	7.52	7.15
EV/EBITDA	-181.08	-277.35	725.92	113.88

数据来源：贝格数据，东吴证券研究所

请务必阅读正文之后的免责声明部分

免责声明

东吴证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本研究报告仅供东吴证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。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，本公司不对任何人因使用本报告中的内容所导致的损失负任何责任。在法律许可的情况下，东吴证券及其所属关联机构可能会持有报告中提到的公司所发行的证券并进行交易，还可能为这些公司提供投资银行服务或其他服务。

市场有风险，投资需谨慎。本报告是基于本公司分析师认为可靠且已公开的信息，本公司力求但不保证这些信息的准确性和完整性，也不保证文中观点或陈述不会发生任何变更，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。

本报告的版权归本公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用、刊发、转载，需征得东吴证券研究所同意，并注明出处为东吴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

东吴证券投资评级标准:

公司投资评级:

买入：预期未来 6 个月个股涨跌幅相对大盘在 15%以上;

增持：预期未来 6 个月个股涨跌幅相对大盘介于 5%与 15%之间;

中性：预期未来 6 个月个股涨跌幅相对大盘介于-5%与 5%之间;

减持：预期未来 6 个月个股涨跌幅相对大盘介于-15%与-5%之间;

卖出：预期未来 6 个月个股涨跌幅相对大盘在-15%以下。

行业投资评级:

增持： 预期未来 6 个月内，行业指数相对强于大盘 5%以上;

中性： 预期未来 6 个月内，行业指数相对大盘-5%与 5%;

减持： 预期未来 6 个月内，行业指数相对弱于大盘 5%以上。

东吴证券研究所
苏州工业园区星阳街 5 号
邮政编码：215021
传真：（0512）62938527
公司网址： http://www.dwzq.com.cn