创新技术与企业服务研究中心

奇安信 (688561.SH) 买入（首次评级）

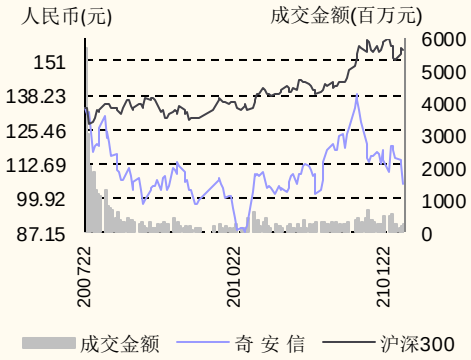
公司深度研究

市场价格（人民币）：104.98 元

新网安领军

市场数据(人民币)

总股本(亿股)	6.80
已上市流通 A 股(亿股)	.73
总市值(亿元)	713.46
年内股价最高最低(元)	139.00/87.15
沪深 300 指数	5485
上证指数	3517



公司基本情况(人民币)

项目	2018	2019	2020E	2021E	2022E
营业收入(百万元)	1,817	3,154	4,191	5,983	8,553
营业收入增长率	121.22%	73.61%	32.86%	42.78%	42.95%
归母净利润(百万元)	-872	-495	-313	-116	156
归母净利润增长率	38.41%	-43.22%	-36.67%	-62.97%	N/A
摊薄每股收益(元)	N/A	-0.86	-0.46	-0.17	0.23
每股经营性现金流净额	N/A	-2.05	-2.47	-1.46	-0.73
ROE(归属母公司)(摊薄)	-20.29%	-9.85%	-3.03%	-1.13%	1.51%
P/E	N/A	N/A	-273.42	-738.32	550.35
P/B	N/A	N/A	8.29	8.38	8.30

来源：公司年报、国金证券研究所

投资逻辑

- **脱胎于三六零集团，高速成长为政企安全龙头。**奇安信自 2015 年从三六零集团分拆以来，凭借着领先安全大数据实力和高举高打的营销策略，2017-2019 年营收年复合增速达 95.98%，迅速成为我国网络安全行业龙头。公司云安全、终端安全、态势感知系统以及安全服务市占率均为行业首位，并在 Gartner 魔力象限中多次处于领导者象限，同时，大量创新赛道产品全面开花，通过产品方案+服务的业务布局，引领行业前进方向。
- **网络安全进入到主动防御新阶段，政策、监管、需求场景和供给侧共同推动行业发展。**政策：网络安全行业受政策影响大，行业延续高景气度。各项政策的落地从覆盖广度、深度、力度等多个维度提高国内网络安全市场投入的积极性，长期带动需求增加。监管：监管合规更注重实战化效果。需求场景旺盛：5G 商用催生大量云大物工等新兴 IT 技术领域的安全需求。预计到 2021 年，云安全、大数据安全、物联网安全、工业互联网安全市场规模合计将达到 715 亿元，年均增速超过 40%。供给侧：创新型厂商的体系化建设能力、实战化方案效果推动行业集中度不断提升。
- **四大核心竞争优势构筑高壁垒，巩固公司网安龙头地位。**1）公司产品线丰富，新安全业务全面布局且具前瞻性。公司上市募集的 54 亿元中有 45 亿元用于新安全产品研发，目前新赛道产品和软件类收入占比持续提升，增速领跑行业增速。2）威胁情报数据库拥有海量安全大数据，助力主动防御体系。公司是首家提出数据驱动安全的网安企业，目前在国内态势感知体系中处于绝对领导地位。3）高研发投入铸就强大的技术壁垒。近三年平均研发费用率接近 45%，高研发进一步巩固公司产品的市场竞争力。4）国家队背景助力公司在政企市场发展。中国电子目前持股 20%，为公司第二大股东，同时，公司成功入局 PKS 生态体系，有望进一步提升政企安全市场份额。

投资建议

- 预计公司 20-22 年营收为 41.91 亿元、59.83 亿元和 85.53 亿元，净利润为-3.13、-1.16、1.56 亿元，采用 PS 估值法，给予公司 22 年市值 1283.02 亿元，对应目标价为 188.68 元，首次覆盖给予“买入”评级

风险提升

- 市场竞争加剧；网络安全政策推进不及预期；商誉减值风险；解禁风险等。

翟炜 分析师 SAC 执业编号：S1130520020005
zhaiwei@gjzq.com.cn

邵广雨 联系人
shaoguangyu@gjzq.com.cn

内容目录

一、从 360 到“国家队”的企业安全平台.....5
1.1 政企安全龙头成长之路.....5
1.2 产品+服务：打造具备内生安全能力的协同联动防护体系.....5
1.3 股权结构：实控人齐向东行业经验丰富，第二大股东中国电子持股 20.26%.....7
1.4 收入高速增长，净利润亏幅加速收窄.....7
二、行业分析：网络安全进入新时代.....9
2.1 政策端：等保 2.0+HW 行动+信创，网安政策持续加码.....9
2.2 需求端一：从被动防护到主动防御，新技术催生千亿级新兴网络安全需求.....14
2.3 需求端二：安全服务需求提升.....17
2.4 供给端：行业集中度不断提升.....18
2.5 客户端：得大客户得天下.....18
三、奇安信核心竞争优势：技术实力强、安全数据丰富、新安全布局、国家队背景.....19
3.1 持续行业高水平研发投入，技术实力雄厚，成果转化率高.....19
3.2 威胁情报数据库拥有海量数据，助力主动防御业务.....21
3.3 产品线丰富，新安全业务布局最全面前瞻.....22
3.4 政府资源丰富，国家队背景助力政企市场持续拓展.....24
四、盈利预测与投资建议.....26
4.1 盈利预测.....26
4.2 投资建议及估值.....27
五、风险提示.....27

图表目录

图表 1：奇安信发展历程.....5
图表 2：奇安信产品与服务体系.....6
图表 3：奇安信网络安全产品分类.....6
图表 4：奇安信代表性软硬一体形态的设备.....6
图表 5：奇安信安全服务布局.....7
图表 6：奇安信重要股东.....7
图表 7：2016-2020Q3 年公司营业收入情况.....8
图表 8：2016-2020Q3 年公司归母净利润情况.....8
图表 9：2017-2019 年网络安全厂商安全业务营收对比.....8
图表 10：2019 年网络安全企业营业收入增长率.....8
图表 11：2017-2019 年公司细分业务毛利率情况.....9
图表 12：2017-2019 公司及行业平均毛利率情况.....9

图表 13：2017-2019 年奇安信与行业竞争对手应收账款周转率情况.....9
图表 14：网络安全行业近期政策汇总.....10
图表 15：等保 2.0 延续五级分级.....11
图表 16：网络安全等级保护工作 5 个步骤.....11
图表 17：定级的变化.....11
图表 18：等保 2.0 定级过程更加规范.....12
图表 19：安全通用要求分类变化.....12
图表 20：等保 2.0 控制点整合后略有缩减.....13
图表 21：等保 2.0 详细要求项略有缩减.....13
图表 22：历年护网行动.....14
图表 23：中国信创产业相关行业概览.....14
图表 24：中美两国网络安全行业发展历程图.....15
图表 25：中国网络安全投入占 IT 总支出比例偏低.....15
图表 26：2016-2020E 中国网络安全市场规模及增速.....15
图表 27：中国云安全、大数据安全、物联网安全、工业互联网安全市场规模16
图表 28：中国网络安全整体市场奇安信份额第一.....17
图表 29：2019 年中国云安全市场奇安信位居第一.....17
图表 30：2017-2019 全球网络安全市场结构.....17
图表 31：2016-2021E 中国网络安全市场结构.....17
图表 32：头部厂商安全服务业务占比.....18
图表 33：2019 年中国网络安全服务市场奇安信份额第一.....18
图表 34：2016-2019 中国网络安全行业集中度情况.....18
图表 35：网络安全产业链上中下游.....19
图表 36：2018 年中国网络安全行业下游构成.....19
图表 37：奇安信客户群体主要包括政府、企业、金融机构等头部客户.....19
图表 38：公司研发费用率和业内其他公司对比情况.....20
图表 39：公司技术人员人数与竞争对手对比情况.....20
图表 40：公司参与组建实验室及研究中心.....20
图表 41：2017-2019 年奇安信技术产业化收入不断增加（单位：亿元）.....21
图表 42：威胁感知系统（天眼）产品架构.....21
图表 43：威胁感知系统（天眼）产品四大能力.....21
图表 44：公司处于中国态势感知解决方案绝对领导者地位.....22
图表 45：公司在安全牛中国网络安全行业全景图中一类安全领域入选情况...22
图表 46：2020 年上半年终端安全软件市场.....23
图表 47：2020 年上半年中国安全分析和威胁情报市场.....23
图表 48：募投资金加码新安全布局.....23
图表 49：奇安信安全产品体系及主要的新安全产品.....24
图表 50：新赛道产品对标新兴领域需求.....24
图表 51：2017-2019 年奇安信新安全产品收入占比不断提升（单位：亿元）24

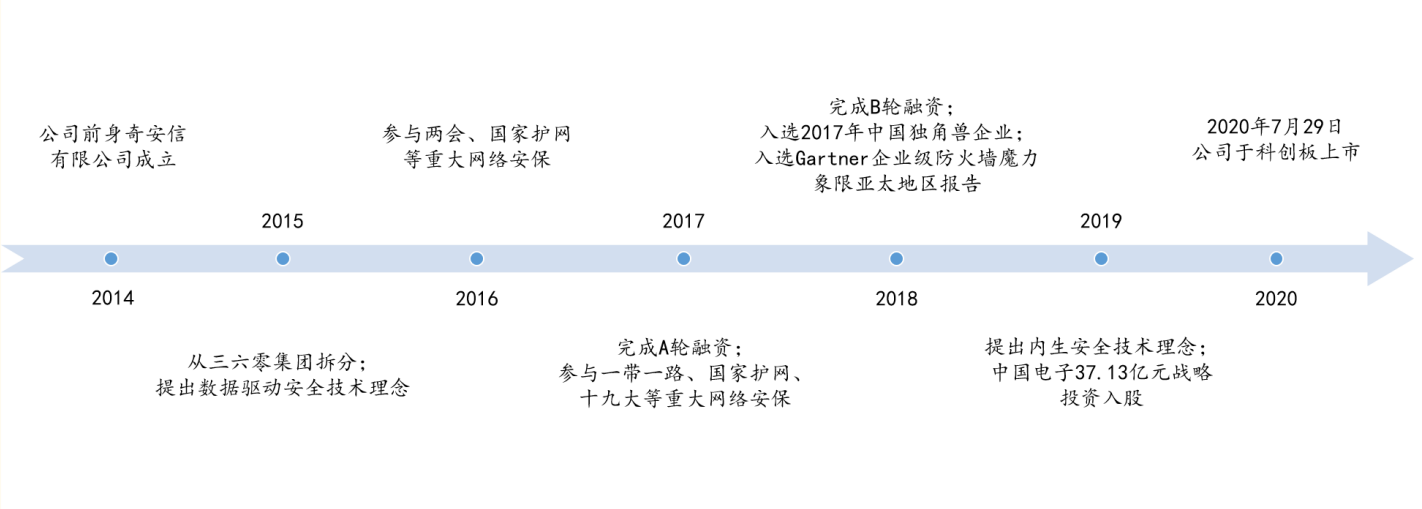
图表 52：2017-2020 年奇安信参与多项重大安保活动.....24
图表 53：2019 年 5 月 10 日，举行中国电子战略入股奇安信发布会.....25
图表 54：飞腾携手麒麟软件打造 PKS 自主可信生态体系.....25
图表 55：公司分业务营收预测（单位：亿元）.....26
图表 56：公司分业务毛利率预测.....26
图表 57： Palo Alto 高速发展期的 PS(TTM)情况.....27
图表 58： CrowdStrike 高速发展期的 PS(TTM)情况.....27
图表 59： Palantir 高速发展期的 PS(TTM)情况.....27
图表 60：Okta 高速发展期的 PS(TTM)情况.....27

一、从 360 到“国家队”的企业安全平台

1.1 政企安全龙头成长之路

- **脱胎于 360 的网络安全公司，风口切入点精准。**2012 年，360 开拓细分市场，开始为企业客户提供 IT 外包和提供集成服务。2014 年奇安信成立，360 将原有的网站安全+企业安全+安全卫士部分业务打包给奇安信，并陆续投资收购了网神信息技术（北京）有限公司、北京网康科技有限公司两家公司。奇安信是 360 在 B 端业务的重要布局，垂直于政企安全 B 端市场。2015 年，360 成立“奇虎 360 企业安全集团”，奇安信安全业务与 360 集团进一步独立。2015 年底，齐向东与周鸿祎签订《关于 360 企业安全业务之框架协议》，齐向东成为奇安信实际控制人。双方约定，周鸿祎控制的企业将主要从事 To C 安全业务，齐向东控制的企业主要从事 To B、To G 安全业务。
- **与 360 分家，中国电子强势入股，奇安信终成“国家队”。**2016 年 7 月，360 美国退市，奇安信也正式从 360 体内分拆出来独立运营。2019 年《终止协议》，将品牌、技术、数据等核心安全能力全部授权收回。同时 360 将股权全部对外转让，根据协议，中国电子以人民币 37.31 亿元持有奇安信 22.59%股份。中国电子成为二股东后，将带动奇安信跻身“国家队”，奇安信政企市场的优势进一步扩大化。
- **深度结合“PK”体系，科创上市引领市场。**奇安信凭借着领先同业的研发投入，仅用了五年便成长为网安行业龙头。并通过与中国电子“PK”体系（飞腾 CPU+麒麟 OS 操作系统）的深度结合，开发出全系列自主创新的安全产品体系。赛迪咨询报告显示奇安信在安全管理平台、终端安全、安全服务以及云安全四大领域的市场占有率均居国内第一。2019 年 6 月，奇安信启动登陆科创板计划；2020 年 6 月奇安信正式成为科创板挂牌交易的国内网络安全“第一股”。

图表 1：奇安信发展历程

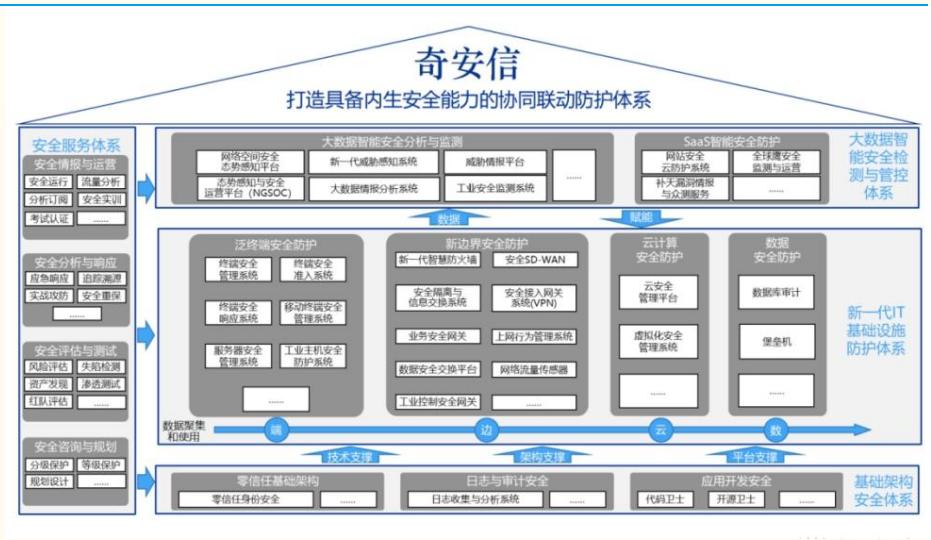


来源：公司官网，国金证券研究所

1.2 产品+服务：打造具备内生安全能力的协同联动防护体系

- **核心业务包括网络安全产品、网络安全服务、硬件及其他业务。**公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务，产品体系覆盖政企行业网络安全的细分领域。

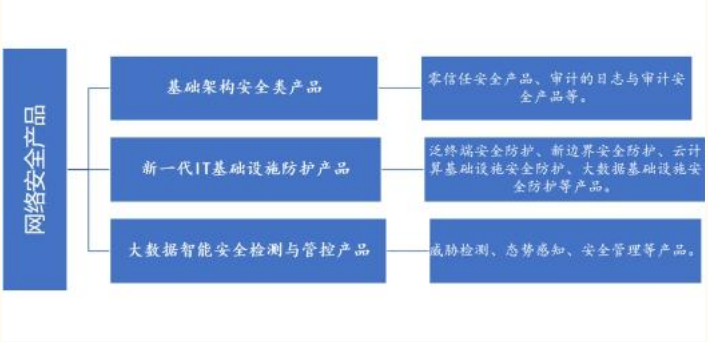
图表 2：奇安信产品与服务体系



来源：公司招股说明书，国金证券研究所

- **网络安全产品：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。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。**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。**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方法，为客户提供检测、感知、分析、响应等能力。

图表 3：奇安信网络安全产品分类



来源：公司官网，国金证券研究所

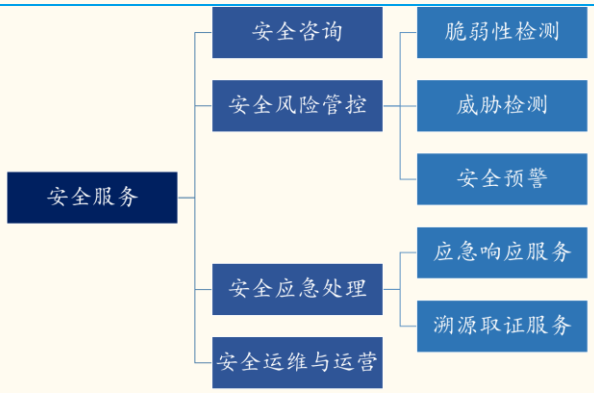
图表 4：奇安信代表性软硬一体形态的设备



来源：公司招股说明书，国金证券研究所

- **网络安全服务：“三同步”打造四大创新安全服务。**“三同步”的原则，即和信息化同步规划、同步建设和同步运行。公司遵循“三同步”的原则，创新发展了规划阶段的安全咨询与规划服务，运行阶段的安全分析与响应服务；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。**安全咨询与规划**包括网络安全体系规划设计、分级保护安全和等级保护安全服务。**安全评估与测试**包括风险评估、失陷检测、资产发现、下一代渗透测试等。**安全分析与响应**包括应急响应服务、追踪溯源服务、实战攻防服务和安全重保服务。**安全情报与运营**包括安全运行、流量分析、订阅分析、安全实训和考试认证服务。

图表 5：奇安信安全服务布局



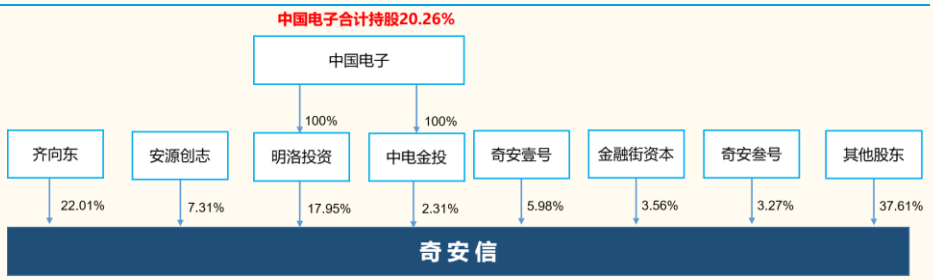
来源：公司官网，国金证券研究所

- **其他硬件采购主要是为客户配套外采第三方硬件产品并销售给对方的业务。**典型的采购内容包括服务器、交换机等 IT 设备并与公司提供给客户的解决方案相结合。该业务主要根据客户需求采购，最近几年奇安信所服务的政企客户信息化改造的综合需求不断增加，公司参与此类项目的数量及规模增长较快。
- **奇安信拥有完善的产品布局，同时具备终端、云端和边界的安全防护能力，兼有强大的安全服务能力，相较于竞争对手，更能给客户提供一站式的安全解决方案。**

1.3 股权结构：实控人齐向东行业经验丰富，第二大股东中国电子持股 20.26%

- **公司实际控制人为齐向东，直接持股 22.01%。**截至到 2020Q3 公司实际控制人、控股股东齐向东先生直接持有公司 22.01%的股权，并通过其控制的安源创志、奇安叁号间接控制公司部分股权，为公司实际控制人。齐向东先生作为奇安信董事长，曾任职新华社通信技术局副局长、三六零集团创始人兼总裁，拥有二十多年的安全行业经验，对行业发展及相关政策导向极具敏感性。
- **中国电子强势入局，持股 20.26%。**2019 年，中国电子通过旗下的明洛投资 37.31 亿元战略入股奇安信，持有公司 17.95%的股份，中国电子的入股使得奇安信正式成为网安国家队之一。由于网络安全行业的特殊性和机密性，国家队背景将为公司在政企领域业务拓展带来助力。

图表 6：奇安信重要股东



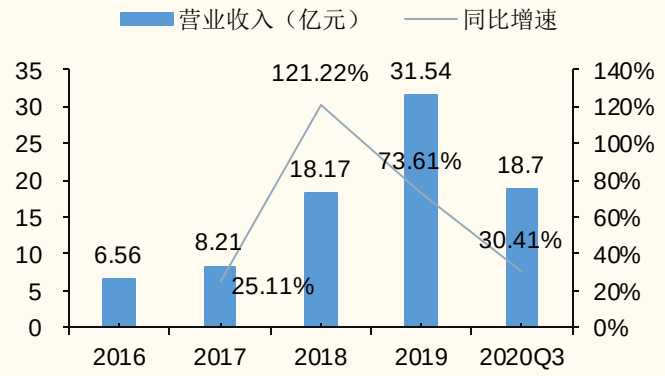
来源：wind，国金证券研究所

1.4 收入高速增长，净利润亏幅加速收窄

- **营业收入飞速增长，盈利能力在连续亏损的情况下大幅改善。**公司 2019 年实现营业收入 31.54 亿元，同比增长 73.61%。2016-2019 年，公司在行业规模持续扩大，品牌效应等因素下，营业收入从 6.56 亿元增长至 31.54 亿元，年复合增长率达到 95.98%，4 年内持续呈现强劲增长趋势。净利润方面，2019 年归母净利润为-4.95 亿元，虽然公司尚未实现盈利，但 2019 年亏损金额较 2018 年同期减少 43.23%，亏损情况显著收窄，盈利能力大幅度改善。公司连续亏损主要是由于为建设四大研发平台、布局新赛道、提升攻防竞争力、建立全国应急响应中心，在研发和销售方面投入巨大。

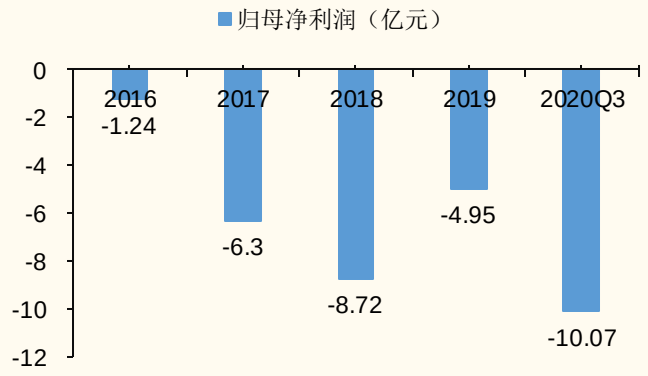
- 最新业绩预告显示，公司 20 年全年预计实现营业收入 41 亿元-42.5 亿元，同比增长 29.99%到 34.75%。实现归母净利润-3.90 亿元到-2.80 亿元，同比亏损减少 21.21%到 43.43%。2020 年公司受疫情影响，仍未实现盈利，但受益于金融、运营商、央企等企业级客户市场增长强劲，以及新赛道产品的成功布局，公司亏损金额持续实现显著收窄。随着公司营收规模加大、经营效率提升、研发平台协同效应显现，有望在未来快速实现扭亏为盈。

图表 7：2016-2020Q3 年公司营业收入情况



来源：wind，国金证券研究所

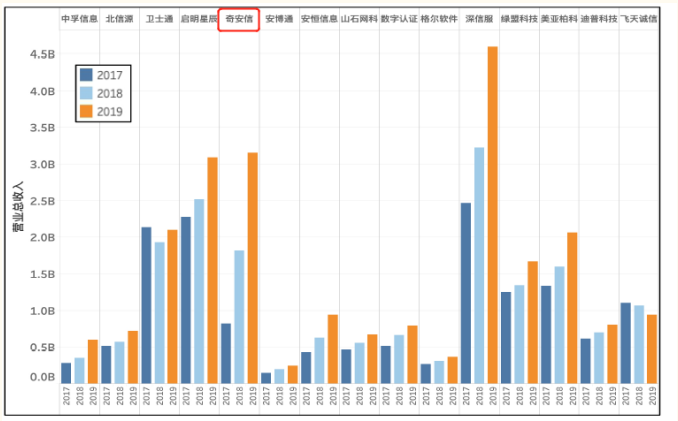
图表 8：2016-2020Q3 年公司归母净利润情况



来源：wind，国金证券研究所

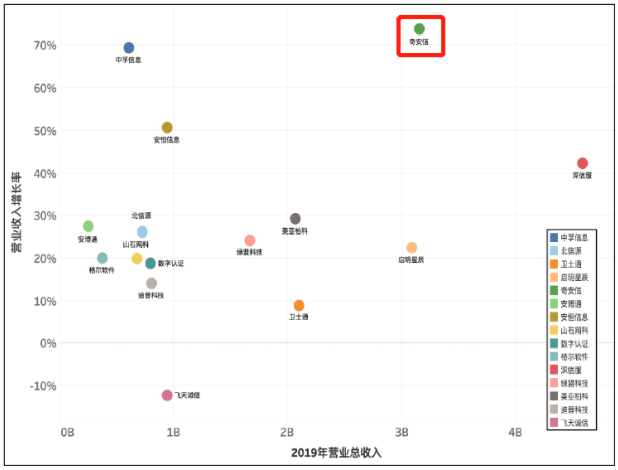
- **同行业比较来看，奇安信营收体量及增速均居行业第一。**2019 年，行业内 15 家典型的网络安全上市公司合计实现营收 227.8 亿元。仅奇安信和启明星辰安全业务收入体量超过 30 亿元，其中，奇安信收入 31.54 亿元，位居行业第一。从收入增速来看，奇安信 2019 年收入达到 73.58%，远超行业内其他厂商。

图表 9：2017-2019 年网络安全厂商安全业务营收对比



来源：中国网络安全产业联盟，国金证券研究所

图表 10：2019 年网络安全企业营业收入增长率

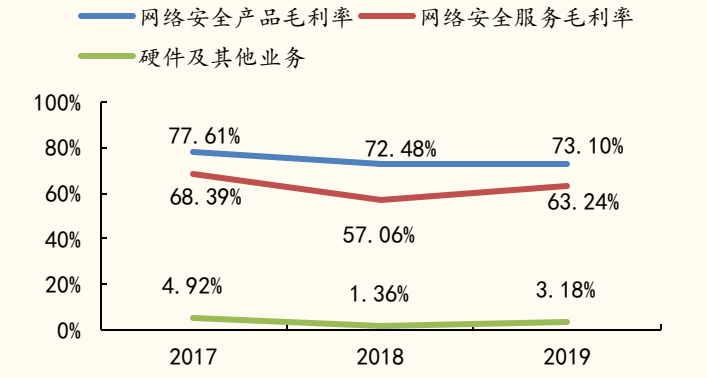


来源：中国网络安全产业联盟，国金证券研究所

- **毛利率分业务来看，网安产品最高，硬件产品最低。**公司网络安全产品市场竞争优势明显，毛利率最高，网络安全服务业务毛利率相对网络安全产品较低，主要由于公司在面向客户提供服务时，一般实施周期较长且需要较多人员投入，是由网络安全行业的行业属性导致。而第三方硬件产品市场目前已经趋于成熟，行业竞争激烈，价格相对较为透明，因此，在公司各项业务中毛利率最低。
- **综合毛利率稳步回升。**2017 年-2020 年 Q3，公司主营业务毛利率分别为 74.39%、55.15%、56.69%及 57.81%，18 年毛利率大幅下降主要是由于公司开始承接较多系统集成性质的网络安全项目，导致毛利率较低的硬件及其他业务收入增长，而 19 年开始，公司在各行业提供的创新攻防演习及安全实训业务竞争优势明显，收入规模增长较快，硬件业务占比下降，毛利率有所提升。

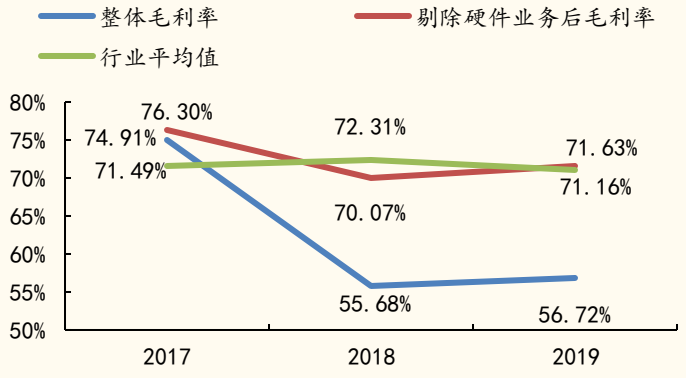
■ **剔除硬件业务后综合毛利率符合行业平均水平。**与行业平均毛利率相比，公司综合毛利率较低，其主要原因在于公司承接较多系统集成性质的网络安全项目，导致毛利率较低的硬件及其他业务收入增速较快。但剔除毛利率较低的硬件业务后，公司网安服务及网安产品的综合毛利率可达 70%以上，核心业务毛利率保持较高水平，符合同行业平均水平。

图表 11：2017-2019 年公司细分业务毛利率情况



来源：wind，国金证券研究所

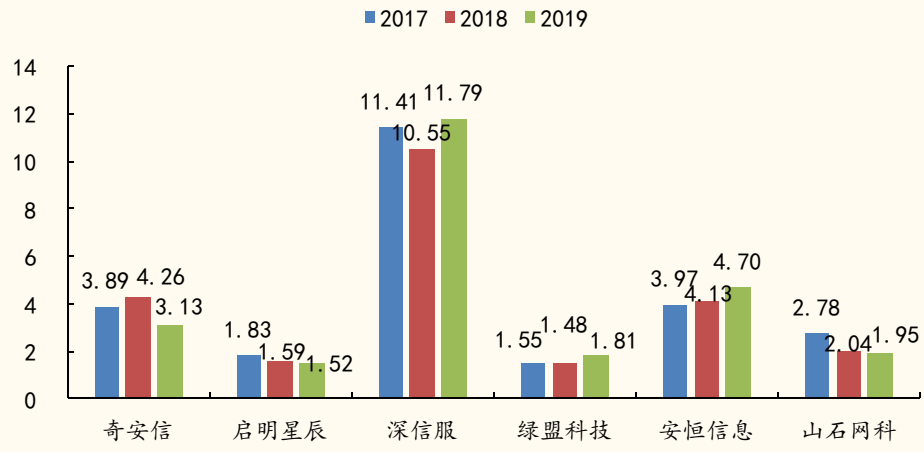
图表 12：2017-2019 公司及行业平均毛利率情况



来源：wind，国金证券研究所

■ **政企客户付款周期长，应收账款周转率偏低。**公司集成类项目最终客户多为政企单位，受其预算管理和集中采购制度等因素影响，付款周期较长，使得公司应收账款较多，应收账款周转率在行业均值左右。但相应的，政企单位的网安预算更稳定充足，坏账较少，尤其在经济遭受疫情风波冲击后，除项目周期延缓外，整体无需多虑。

图表 13：2017-2019 年奇安信与行业竞争对手应收账款周转率情况



来源：wind，国金证券研究所

二、行业分析：网络安全进入新时代

2.1 政策端：等保 2.0+HW 行动+信创，网安政策持续加码

■ **政策利好行业快速发展。**网络安全行业属于下游驱动型行业，且政府占据下游客户端中的主导地位。近年来，随着国家对网络安全的重视程度逐渐提高，网信办等政府部门围绕网络安全陆续出台了多项法律法规。国家监管环境的变化以及大量政策的出台，均提升了客户对于安全服务的重视程度，持续强劲驱动行业发展。此外，近期疫情得到控制后，网络安全行业正在加快全面恢复，下游需求景气度明显提升。

图表 14：网络安全行业近期政策汇总

时间	部门	文件	主要内容
2016.11	全国人大常委会	《中华人民共和国网络安全法》	保障网络安全，维护网络空间主权及国家安全，保护公民合法权益，促进经济社会信息化发展。
2018.03	网信办、工信部	《关于推动资本市场服务网络强国建设的指导意见》	加快扶持网信企业在资本市场中的融资能力，鼓励网信企业并购重组，完善产业链条。
2019.05	市场监督管理总局	《网络安全等级保护基本要求》《网络安全等级保护测评要求》	网络安全领域规范性条例，指导性及强制力度较大，明确了网络安全等级保护2.0的核心标准，确立了云计算、移动互联网、物联网以及工业控制系统的安全要求。
2019.07	工信部、教育部	《加强工业互联网安全工作的指导意见》	指明工业互联网安全保障体系将于2020年底初步建立，到2025年逐步完善制度，工业互联网领域安全产业规模化发展，基本建立起完善的工业互联网保障体系。
2019.09	工信部	《关于促进网络安全产业发展的指导意见》	到2025年，培育一批年营收超过20亿元的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，2025年网络安全产业预计将超过2000亿元。
2019.10	全国人大常委会	《中华人民共和国密码法》	规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，是中国密码领域的综合性、基础性法律。
2019.12	公安部	《网络安全等级保护条例》	扩大了保护对象的范围、丰富了保护方法、增加了技术标准。将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、等工作措施全部纳入等级保护制度。
2020.03	信息安全标委会	《网络安全标准实践指南—远程办公安全防护》	针对远程办公系统使用方和用户分别提出了安全控制措施建议，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。
2020.04	网信办等12部门	《网络安全审查办法》	通过网络安全审查这一举措，保障关键信息基础设施供应链安全，维护国家安全，为我国开展网络安全审查工作提供了重要的制度保障。
2020.05	工信部	《关于工业大数据发展的指导意见》	提出促进工业数据汇聚共享、融合创新，提升数据治理能力，加强数据安全管理，着力打造资源富集、应用繁荣、产业进步、治理有序的工业大数据生态体系。
2020.06	十三届人大常委会	《中国人民共和国数据安全法（草案）》	确立数据分级分类管理以及风险评估，检测预警和应急处置等数据安全管理各项基本制度；落实数据安全保护责任；建立保障政务数据安全和推动政务数据开放的制度。
2020.07	工信部	《工信部和信息化部办公厅关于开展2020年网络技术应用试点示范工作的通知》	试点重点方向包括新型信息基础设施安全类：5G网络安全、工业互联网安全、车联网安全、智慧城市安全、大数据安全、物联网安全、人工智能安全、区块链安全等。

来源：工信部，网信办，公安部，国金证券研究所

- **（1）等保2.0促进主动安全防御需求增加，网安需求更盛**

- 2019年5月13日，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》**三项国家标准正式发布**，并于2019年12月1日正式实施。

  上述三项政策构成我国网络安全等级保护2.0制度（简称等保2.0），等保2.0是我国网络安全领域的基本国策、基本制度。与等保1.0相比，等保2.0延续了五个级别的划分，五个级别依次是：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

图表 15：等保 2.0 延续五级分级



来源：安全牛，国金证券研究所

■ 网络安全等级保护工作包括定级、备案、安全建设、等级测评、监督检查五个步骤，相较于等保 1.0，等保 2.0 的五个步骤里发生了较多变化。

图表 16：网络安全等级保护工作 5 个步骤

定级	**确定定级兑现，参考指南等初步确定登记，组织专家评审，主管单位审核，公安机关备案审查。**
备案	持定级报告和备案表等材料到公安机关网安部门进行备案。
安全建设	以要求中对应登记的要求为标准，对定级对象当前不满足要求的进行建设整改。
等级测评	委托具备测评资质的测评机构对定级对象进行等级测评,形成正式的测评报告。
监督检查	向当地公安机关网安部门提交测评报告,配合完成对网络安全等级保护实施情况的检查。

来源：深信服官网，国金证券研究所

■ **定级的变化：**

- 定级对象变化，等保 1.0 定级的对象是信息系统，等保 2.0 的定级对象向“云移物工大”扩展，基础网络、重要信息系统、互联网、大数据这些、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务器平台等都纳入了等保 2.0 的保护范围。
- 定级级别的变化：公民、法人和其他组织的合法权益产生特别严重损害时，相应系统的等级保护级别从 1.0 时代的的第二级调整到了第三级。

图表 17：定级的变化

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

来源：创宇云安全，国金证券研究所

- 定级流程的变化：不同于等保 1.0 定级原则“自主定级、自主保护”，等保 2.0 则采取了专家评审，主管部门审核的方式，定级过程将会变得更加规范，定级也会更加准确。原有的 30 天内备案缩短为 10 个工

作日，并明确了定级流程分为：确定定级对象、初步确定等级、专家评审、主管部门审核、公安机关备案。

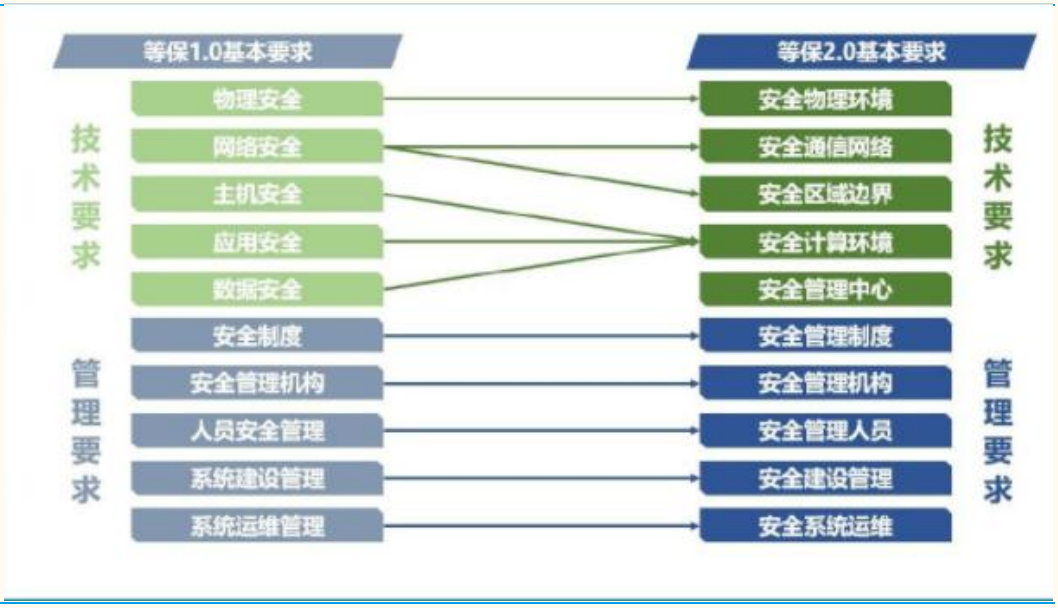
图表 18：等保 2.0 定级过程更加规范



来源：创宇云安全，国金证券研究所

- **等级测评的变化：**
  - 测评合规要求提高：相较于等保 1.0，等保 2.0 测评的及格分从 60 分上调到了 75 分。
  - 安全要求扩展：安全要求由 1.0 时代的基本要求扩展成为安全通用要求+安全扩展要求，新增扩展要求包括云计算、移动互联网、物联网、工业控制、大数据安全。其中通用要求不管等级保护对象的形态如何均需要满足，而其他扩展要求针对不同的 IT 基础设施。
  - 测评周期变短：由原来的四级系统每半年需要测评一次改为三级以上系统一年测评一次。
  - 测评要求发生变化：以通用类要求为例，首先在要求分类上发生变化，安全管理要求被纳入技术要求中。

图表 19：安全通用要求分类变化



来源：百度文库，国金证券研究所

其次对应具体的控制点和要求项也发生了变化，等保 2.0 对等保 1.0 的控制点和要求项进行了优化，删除或修订了过时的要求项，新增了对新型网络攻击行为防护和个人信息保护等内容。从数量上看，等保 2.0 的控制点和要求项相对于等保 1.0 都有所减少，但实际上 2.0 标准的覆盖面比 1.0 标准要更广，要求也要高得多。主要体现在：一方面等保 2.0 标准将原来 1.0 标准的不同层面的相同要求项进行了合并，如主机、数据库、网络设备的要求，所以新标准的一个要求项往往覆盖了老标准的多个要求项；另一方面很多要求项的要求更高了，覆盖面更大了，比如针对网络入侵防范，新规定明确要求对关键节点要具有内部和外部的攻击检测能力（1.0 仅要求网络边界处的检测能力）；

同时如果定级对象使用了云计算、大数据等新技术，那么还需考虑扩展要求的内容。

图表 20：等保 2.0 控制点整合后略有缩减

等保1.0	控制类	二级	三级	四级	等保2.0	控制类	二级	三级	四级
技术要求	物理安全	10	10	10	技术要求	安全物理环境	10	10	10
	网络安全	6	7	7		安全通信环境	3	3	3
	主机安全	6	7	9		安全区域边界	6	6	6
	应用安全	7	9	11		安全计算环境	10	11	11
	数据安全	3	3	3		安全管理中心	2	4	4
安全管理	安全制度	3	3	3	安全管理	安全管理制度	4	4	4
	安全管理制度	5	5	5		安全管理机构	5	5	5
	人员安全管理	5	5	5		安全管理人员	4	4	4
	系统建设管理	9	11	11		安全建设管理	10	10	10
	系统运维管理	12	13	13		安全系统运维	14	14	14
合计		66	73	77	合计		68	71	71

来源：百度文库，国金证券研究所

图表 21：等保 2.0 详细要求项略有缩减

等保1.0	控制类	二级	三级	四级	等保2.0	控制类	二级	三级	四级
技术要求	物理安全	19	32	33	技术要求	安全物理环境	15	22	24
	网络安全	18	33	32		安全通信环境	4	8	11
	主机安全	19	32	36		安全区域边界	11	20	21
	应用安全	19	31	36		安全计算环境	23	34	36
	数据安全	4	8	11		安全管理中心	4	12	13
安全管理	安全制度	7	11	14	安全管理	安全管理制度	6	7	7
	安全管理制度	9	20	20		安全管理机构	9	14	15
	人员安全管理	11	16	18		安全管理人员	7	12	14
	系统建设管理	28	45	48		安全建设管理	25	34	35
	系统运维管理	42	62	70		安全系统运维	31	48	52
合计		176	290	318	合计		135	211	228

来源：百度文库，国金证券研究所

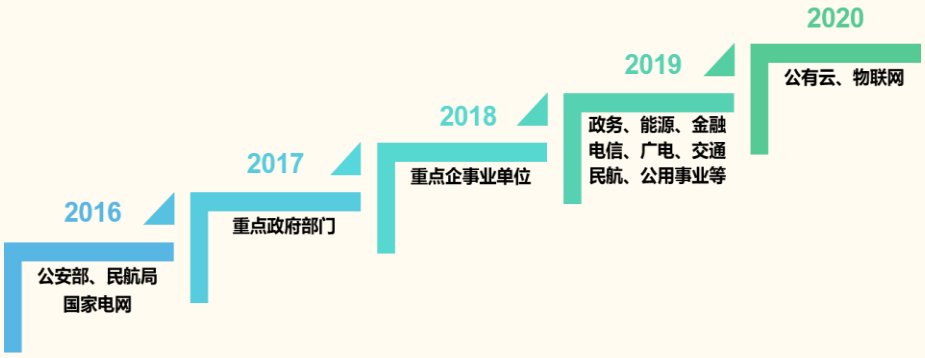
- 总体而言，新时期国家网络安全等级保护制度具有鲜明特点：一是覆盖各地区、各单位、各部门、各企业、各机构，也就是**覆盖全社会**，除个人及家庭自建网络的全覆盖；二是**覆盖所有保护对象**，等级保护 1.0 的基本要求中只有普适性的安全要求，等级保护 2.0 则在满足共性安全保护需求的安全通用要求基础上，针对**云计算、移动互联、物联网、工业控制**等新技术、新领域提出了安全扩展要求；三是测评难度加大、测评工作量增加、测评标准更高，系统运营使用单位须在系统建设和整改过程中进一步提升安全防护能力；四是等保 2.0 标准采用了**“一个中心、三重防护”**的理念，**从等保 1.0 标准被动防御的安全体系转变为等保 2.0 标准的事前预防、事中响应、事后审计的动态保障体系，注重全方位主动防御、安全可信、动态感知和全面审计，将有望带动威胁情报、态势感知等主动防御产品的需求增加。**

- **（2）HW 行动推动网络安全技术标准建设，助推行业向前发展**

- **HW 行动逐年加码，为行业带来推动力量。**实战攻防演习是新形势下的关键信息基础设施网络安全保护工作的重要组成。近年来，公安部定期组织关键信息基础设施运营者进行网络安全攻防实战化演习，提高关键信息基础设施应对网络安全事件的水平和协同配合能力。2016 年开始，实战化攻防演习行动覆盖客户群的横向和纵向都在逐步扩大，攻击手段更加复杂，暴露防守问题更加直接。同时，监管力度也从公安部升级为国务院，表明国家层面对网络安全的重视程度正逐步加深。随着攻防实战化演习慢慢常态

化，其已经成为全行业安全监管的重要抓手，成为企业精准评估自身潜在脆弱性、验证安全防护是否健全的首选方案。由于企业客户可以通过实战化演习看到产品的防护效果以及发现自身安全防护能力的不足。因此，HW行动可以激发客户对网安产品的购买意愿，助推行业需求提升。

图表 22：历年护网行动



来源：任子行，国金证券研究所

- **（3）信创强化网络安全高要求**
- **信创聚焦安全可控，网安行业直面政策东风。**信创产业，即信息技术应用创新产业，包含从 IT 底层的基础软硬件到上层的应用软件全产业链的安全可控。在新的国际形势下，网络安全与国家安全息息相关，网络安全需求将进入井喷式增长期
  - **《“十三五”国家信息化规划》**提出，到 2020 年“数字中国”建设取得显著成效，信息化能力跻身国际前列，具有国际竞争力、安全可控的信息产业生态体系基本建立。受疫情影响，本该处于关键冲刺期的 2020 年进度停缓，因此信创发展带来的网安需求将顺延至 2021 年，2021 年或将成为新的冲刺年。
  - **《国家信息化发展战略纲要》**明确，到 2025 年根本改变核心关键技术受制于人的局面，形成安全可控的信息技术产业体系；到 21 世纪中叶，信息化全面支撑富强民主文明和谐的社会主义现代化国家建设，网络强国地位日益巩固。
  - **“十四五”**将是数字化战略的转型建设关键阶段，国家聚焦关键领域的“安全可靠”、“自主可控”，网络安全产业在未来五年都将处于良好的发展态势。

图表 23：中国信创产业相关行业概览



来源：前瞻产业研究院，国金证券研究所

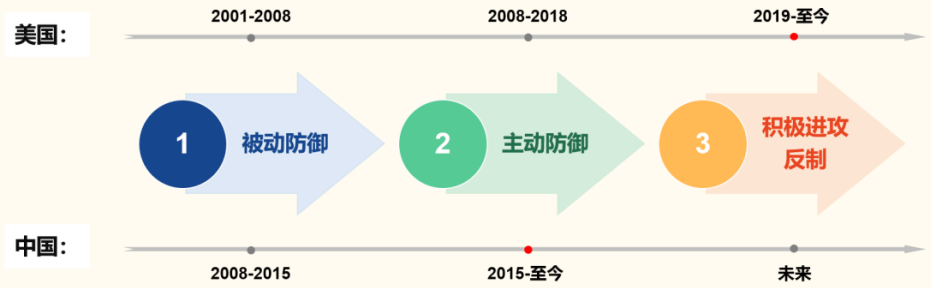
2.2 需求端一：从被动防护到主动防御，新技术催生千亿级新兴网络安全需求

- **美国网络安全行业现已发展至积极进攻反制阶段。**通过参照美国网络安全行业的发展情况，我们可以发现，美国的网络安全建设发展路径是由被动

防御-主动防御-积极进攻反制三个阶段构成的。2001-2008 年，911 事件后，美国开始在各行业布置防火墙、IPS、IDS 等基础安全设施，处于完成基础防御铺设的被动防御时期。2008 年-2018 年，美国历时十年布置了基于安全基础设施、安全大数据的整体网络空间态势感知的防护体系，以国家为中心进行网络安全防护，进入主动防御阶段。2019 年开始，美国政府成立网络司令部，基于其安全大数据属性可以预判到将要发生的攻击，并提前布局积极进攻以实现反制。

- **从被动防御到主动防御，我国网络安全进入新阶段。**尽管我国网络安全行业对于美国而言起步较晚，但两者发展历程是相似的。当前我国已经进入从被动防御升级至主动防御的转换阶段。被动防御时期的传统安全产品部署相对比较基础、简单，部署的各部分安全硬件产品之间比较孤立、缺乏联动，因此难以实现完整全面的安全防护，存在硬伤，迫切需要从被动防御升级转换为主动防御阶段。等保 2.0 政策中也指出，网络安全防护思路要变被动防御为主动防御、纵深防御，并实现全部领域的覆盖。因此，**我们认为，国内网络安全行业的短期目标是把各个行业的安全基础设施能力补齐，以便于获得更全面的安全大数据，并以此为基础进行中上层的能力建设，这也将大大加速网络安全行业的发展。**

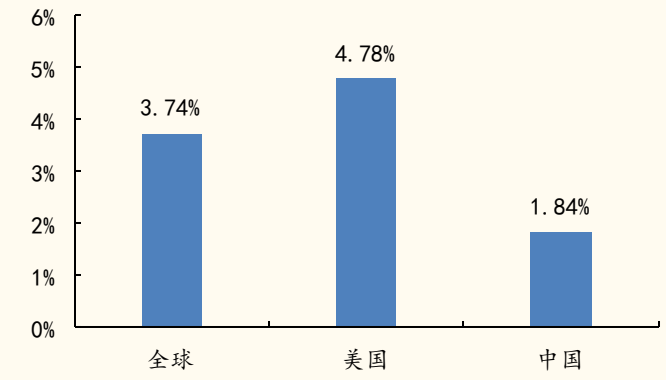
图表 24：中美两国网络安全行业发展历程图



来源：国金证券研究所制

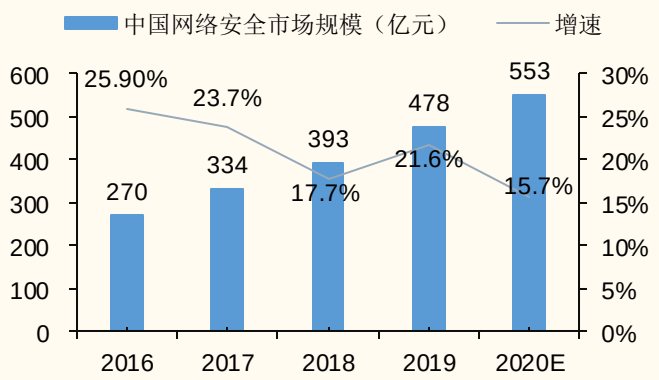
- **对标美国，我国网络安全市场有数倍的成长空间。**2017 年我国安全投入占 IT 总支出的比重为 1.84%，相比于全球市场 3.74%和美国市场 4.78%的占比严重偏低。假设我国未来安全投入占 IT 总支出比重能达到美国的水平，同时考虑我国 IT 总支出仍在快速增长，我国的网络安全市场尚有三到四倍的增长空间。

图表 25：中国网络安全投入占IT 总支出比例偏低



来源：中国产业信息网，国金证券研究所

图表 26：2016-2020E 中国网络安全市场规模及增速



来源：中国安全产业联盟，国金证券研究所

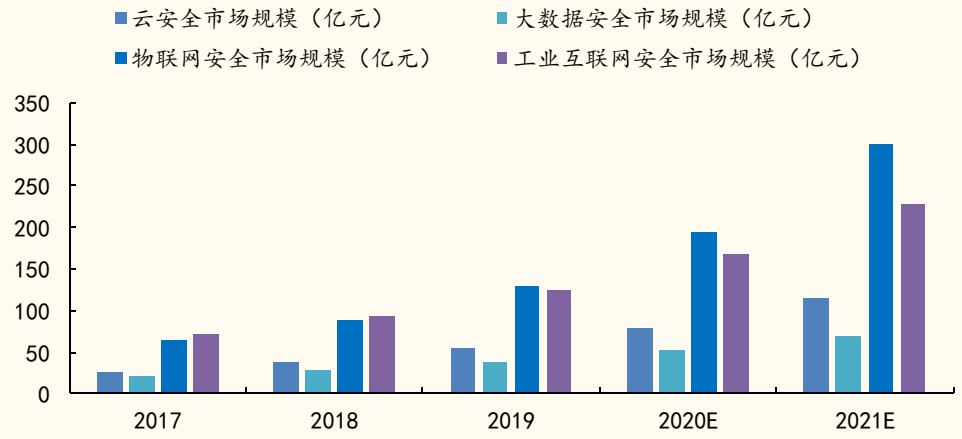
- **安全行业除了由被动防护向主动防御过度外，随着 5G 落地，云计算、大数据、物联网等新技术催生了各类新安全需求。**

- **R16 技术标准固定，5G 行业应用加速落地。**2020 年 7 月，国际标准组织 3GPP 宣布 5G R16 标准正式冻结，标志着 5G 第一个演进版本标准完成。R16 标准不仅增强了 5G 的功能，催生新的数字生态产业，而且在网络能力扩展、挖潜以及降低运营成本等方面进行了改进，实现了高连接速率、超低网络延时、海量终端接入、高可靠性等性能。多场景下 5G 应用落地，将进一步强化网络安全中主动防御的重要性。

- **云、大数据、物联网、工业互联网等技术应用带来安全挑战。**R16 标准的冻结将推动 5G 在 ToB 端应用加速，随着 5G 技术的成熟，云计算、大数据、工业互联网、物联网等行业应用场景加速落地。5G 的应用拓宽了计算边界，将计算场景向外延伸，突破原有市场，新场景下的网络安全产业空间逐渐形成。除此之外，云计算、大数据、工业互联网、物联网等技术需要强大的算力支撑，保障以上技术顺利、安全运行所需的网络安全服务的量级和复杂程度均大幅上升。

- **新技术催生新兴安全需求，市场空间超 700 亿元。**赛迪咨询数据显示，2019 年我国云安全服务市场规模达 55 亿元，大数据安全市场规模 38 亿元，物联网安全市场规模 129 亿元，工业互联网安全市场规模在 125 亿元左右。预计到 2021 年，云安全服务市场规模达 116 亿元，大数据安全市场规模达到 70 亿元，物联网安全市场规模将超过 300 亿元，工业互联网安全市场规模将达到 230 亿元，总体达到 715 亿元。以上几种场景下的安全服务市场规模三年内增长均超过 200%，保障新兴技术安全已成为必然趋势，未来增量市场空间有望达千亿级。

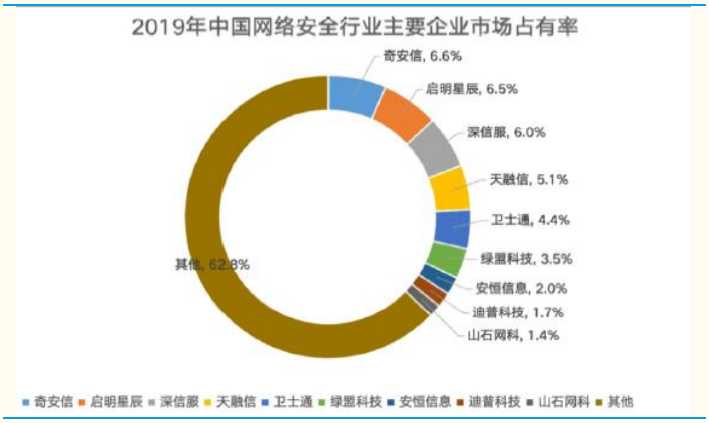
图表 27：中国云安全、大数据安全、物联网安全、工业互联网安全市场规模



来源：赛迪顾问，国金证券研究所

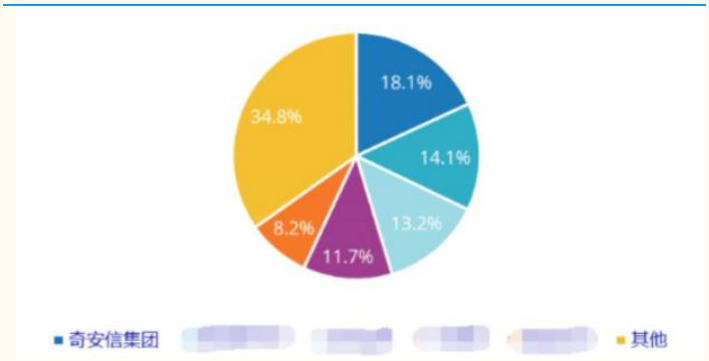
- **奇安信在中国整体网络安全市场和云安全细分市场份额均为第一。**中国安全产业联盟数据显示，2019 年，奇安信、启明星辰和深信服占据国内安全市场营收前三甲，三家公司的市场占有率均达到或超过了 6%，其中奇安信份额为 6.6%，位居行业第一。在云安全市场，2020 年 7 月 IDC 首次发布《中国安全资源池市场份额，2019：新市场、新动能、新发展》研究报告显示，中国安全资源池市场中，奇安信云安全管理平台凭借 18.1% 的市场份额，位列国内第一名。

图表 28：中国网络安全整体市场奇安信份额第一



来源：中国安全产业联盟，国金证券研究所

图表 29：2019 年中国云安全市场奇安信位居第一

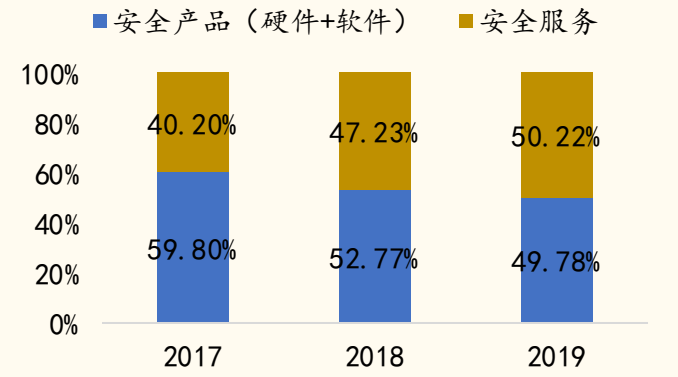


来源：IDC，国金证券研究所

2.3 需求端二：安全服务需求提升

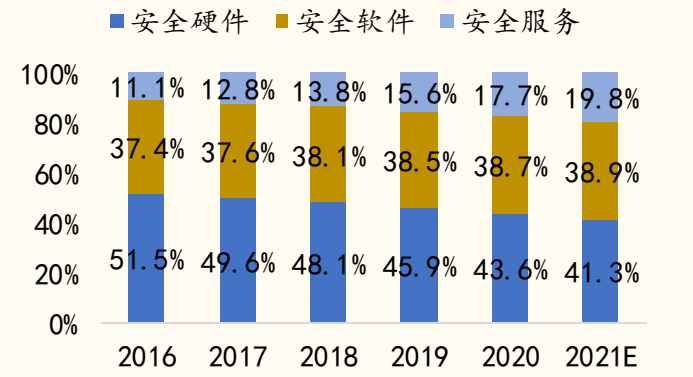
■ **云计算、大数据等新兴技术，推动网络安全服务市场加速发展。**网络安全行业从结构上看，主要分为安全产品（安全硬件和安全软件）和安全服务。长期以来，安全服务作为安全产品的附加品，其重要性及价值被严重低估。但随着云计算技术的普及应用，云安全能力日益受到重视，云防火墙、云审计、DDoS 攻击防御等云化产品快速发展，网络安全服务化的价值逐步得到认可，基于自动化、远程化、智能化的威胁监测、威胁情报等新兴模式逐步试点应用。网络形态的转变，倒逼安全产品加速向服务形态转型，步入软件定义的时代，也将催生出更加繁荣的安全服务市场。目前全球网络安全市场中网络安全服务占比约 50%，而中国市场中安全产品占比超 80%，而安全服务不足 20%，虽然 2016 年以来安全服务比例不断提升，但整体安全服务市场仍有较大增长空间。2020 年 12 月，IDC 数据显示，2020 上半年中国网络安全服务市场厂商整体收入约为 5.72 亿美元（约合 40.23 亿元人民币），厂商收入规模较去年同期下降 27.7%。

图表 30：2017-2019 全球网络安全市场结构



来源：Gartner，国金证券研究所

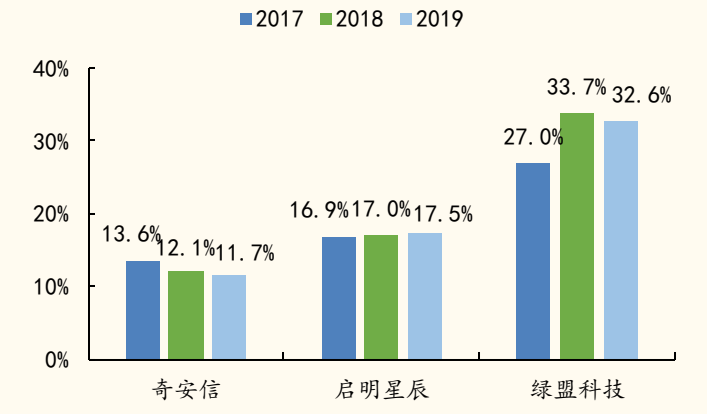
图表 31：2016-2021E 中国网络安全市场结构



来源：赛迪咨询，国金证券研究所

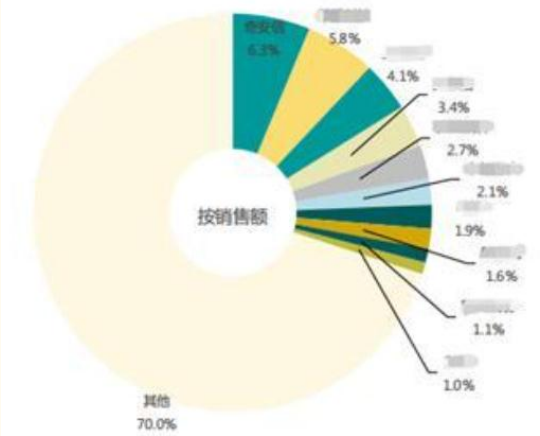
■ **行业头部厂商加速布局网络安全服务，头部效应日益显现。**随着安全即服务理念的不断深入，网络安全头部厂商奇安信、启明星辰、绿盟科技等加快布局网络安全服务业务，2017-2019 年启明、绿盟等老牌网络厂商的网络安全服务业务占比不断提升，而奇安信由于整体业务规模增速飞快，导致网络安全服务业务增速不及整体增速，占比呈下降趋势，但网络安全服务业务收入绝对值高，3 年复合增速达 81%。赛迪咨询数据显示，2019 年我国网络安全服务市场增速为 24.2%，规模达到 73.4 亿元。其中，奇安信以 6.3%的份额领跑市场，位居安全服务市场第一位。因此，我们认为，未来随着网络安全服务市场的快速增长，具有先发优势和服务经验的头部厂商的市场份额有望进一步提升。

图表 32：头部厂商安全服务业务占比



来源：wind，国金证券研究所

图表 33：2019 年中国网络安全服务市场奇安信份额第一

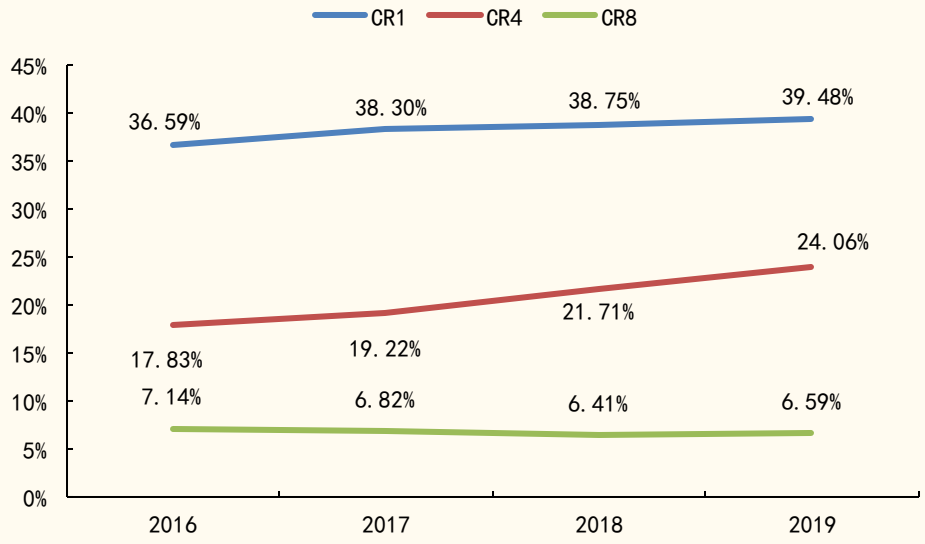


来源：赛迪咨询，国金证券研究所

2.4 供给端：行业集中度不断提升

- **我国网络安全行业已进入低集中寡占型，头部集中趋势明显。**观察美国网络安全行业发展历程可以知道，当网络安全市场进入稳健增长阶段后，头部企业凭借在规模和资源上较大的优势，其市场份额会不断扩大，从而使得网络安全行业集中度将进一步提升。而以奇安信为代表的创新型厂商拥有体系化的建设能力和实战化方案效果，在当前我国网安行业由被动防护想主动防御的阶段转换的过程中，有望持续推升行业集中度。中国网络安全产业联盟数据显示，2019 年我国网络安全市场集中度 CRn 的 CR1 即奇安信的市场份额为 6.59%，CR4 为 24.06%，CR8 为 39.48%。市场集中度的三项指标与 2018 年相比均有一定程度的提升。根据美国经济学家贝恩对产业集中度的划分标准，我国网络安全行业 CR8 基本达到了 40%的水平，表明我国网络安全市场已经由竞争型转变为低集中寡占型，未来行业集中度有望进一步提升。

图表 34：2016-2019 中国网络安全行业集中度情况



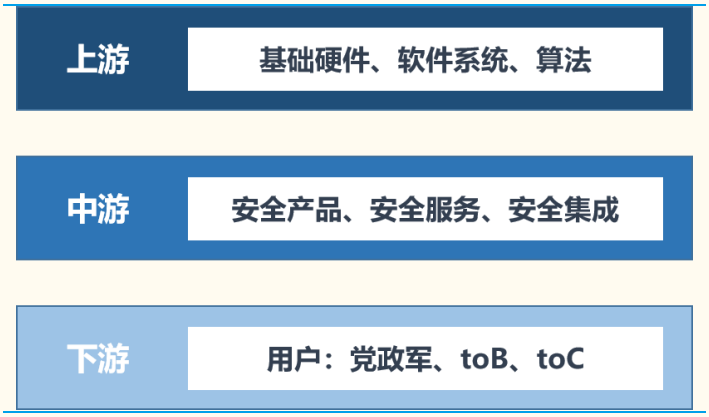
来源：中国网络安全产业联盟，国金证券研究所

2.5 客户端：得大客户得天下

- **网络安全行业为下游驱动型，党政军及行业客户占比有望达到 70%。**从下游客户角度看，网络安全市场的客户从上至下可以划分为国家安全市场、行业安全市场和商业企业客户群。首先，政府端大国在网络空间上的竞争日益加剧，国家对网络安全的重视也逐渐加深，特别是党政军等领域网络

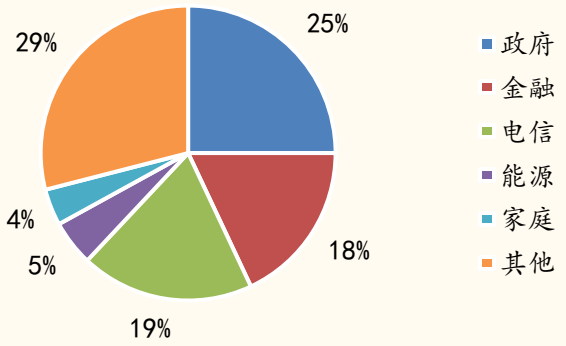
安全支出不断增大。行业端，随着信息安全问题的凸显、网络威胁的发生以及企业自身发展的需要，下游用户对 IT 系统建设的重视和信息安全方面的投入，对信息安全行业的发展具有一定促进作用。金融、电信等行业是国家重点支持发展信息化建设的行业，对信息安全有较高的技术要求和较大的产品需求，该类用户的信息安全需求对信息安全行业的发展具有较大的促进作用。我们认为未来国家安全加行业安全占 70%，商业企业市场则占 30%。因此，网络安全市场拥有典型的“得大客户者得天下”的特点。

图表 35：网络安全产业链上中下游



来源：中国信通院，国金证券研究所

图表 36：2018 年中国网络安全行业下游构成



来源：中国产业信息网，国金证券研究所

- **奇安信在政企等大客户中拥有较大优势。**2019 年，奇安信所有客户中的党政军及重点行业等头部客户比例达到 77.89%，在政企中拥有较大优势。另外，从覆盖率方面来看，截至到 2020Q3，奇安信在党政部委的客户覆盖率达到 95%以上。

图表 37：奇安信客户群体主要包括政府、企业、金融机构等头部客户

行业	2017		2018		2019	
	金额	占比	金额	占比	金额	占比
政府	2.85	35.39%	8.06	44.88%	9.00	28.59%
公检法司	0.72	8.91%	1.97	10.98%	5.32	16.89%
军队军工	0.76	9.47%	1.67	9.29%	2.09	6.64%
能源	0.41	5.05%	0.68	3.77%	2.04	6.49%
金融	0.39	4.87%	0.93	5.17%	1.63	5.17%
教育	0.48	6.01%	0.80	4.48%	1.60	5.07%
医疗卫生	0.35	4.41%	0.78	4.35%	1.51	4.80%
运营商	0.32	3.94%	0.55	3.06%	1.34	4.24%
党政军+重点行业合计	**6.28**	**78.05%**	**15.43**	**85.98%**	**24.53**	**77.89%**

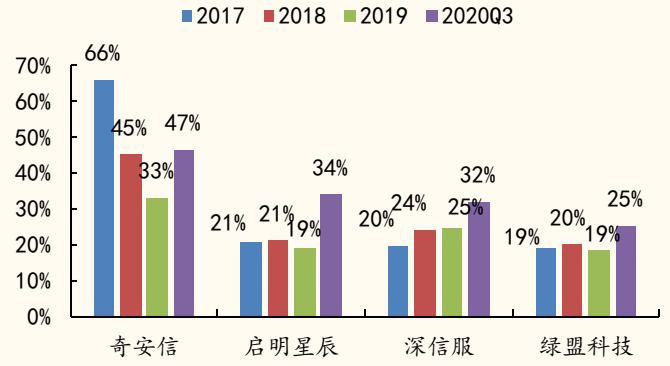
来源：公司招股说明书，国金证券研究所

三、奇安信核心竞争优势：技术实力强、安全数据丰富、新安全布局、国家队背景

3.1 持续行业高水平研发投入，技术实力雄厚，成果转化率高

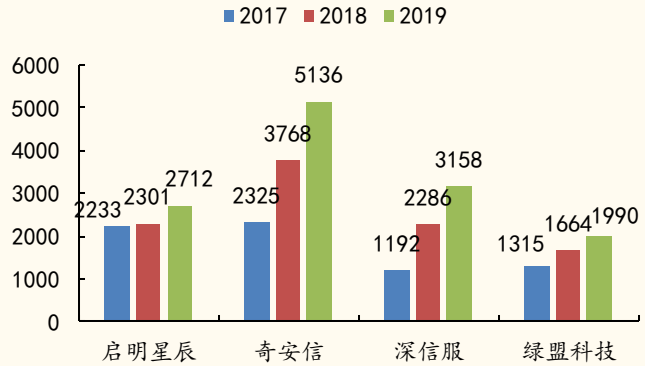
- **研发投入占比行业领先。**2017-2020Q3，奇安信的研发费用率分别达到 65.86%、45.04%，33.20%，46.56%，远高于行业其他竞争对手。
- **庞大的技术人才队伍，助力公司巩固技术壁垒。**从研发人数上看，截至 2019 年年末，公司研发团队人数达到 2591 人，技术支持服务人员数量达 2545 人，技术人员总数达 5136 人。2017-2019 年，技术人员占比始终维持在 70%以上，远远高于同行业其他公司。技术人员占比高表明公司注重核心团队建设，已形成技术人才壁垒。公司通过研发投入的不断加码以及大量研发人才的加入，将高研发投入有效转化为公司强大的技术壁垒，助力公司进一步巩固市场优势。

图表 38：公司研发费用率和业内其他公司对比情况



来源：wind，国金证券研究所

图表 39：公司技术人员人数与竞争对手对比情况



来源：wind，国金证券研究所

- 此外，截至 2020 年 4 月 29 日，公司已拥有 368 项网络安全领域的主要发明专利和 652 项主要计算机软件著作权，另有超过 850 项专利申请正在审核中。此外，公司牵头承建多个国家级和省级工程实验室，同国内顶尖高校及研究所共建学术研究中心，与行业龙头单位建设联合研究机构，共同积极推动我国网络安全行业技术创新。

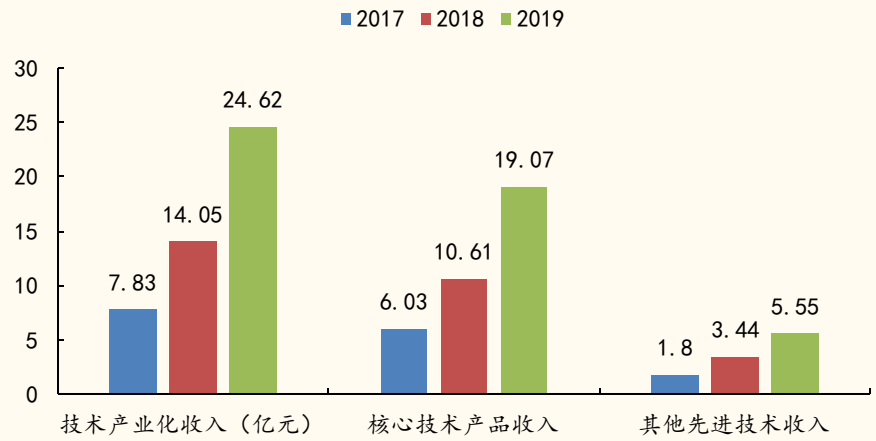
图表 40：公司参与组建实验室及研究中心

	实验室及研究中心
技术研究	牵头承建了“工业控制系统安全国家地方联合实验室”、“工业控制系统安全北京市工程实验室”、“网络安全监测预警关键技术北京市工程实验室”和“应对新兴威胁的高性能应用层防火墙技术北京市工程实验室”等多个国家级和省级实验室
学术研究	与高校共建“清华大学-奇安信网络安全联合研究中心”、“北大-奇安信区块链安全实验室”、“中科院信工所-奇安信网络安全联合实验室”、“中科院软件所-奇安信智能软件安全研究中心”、“广州大学-奇安信云安全联合实验室”、“国科大-奇安信联合实验室”、“天津大学-奇安信网络空间安全研究院”、“哈工大（深圳）-奇安信数据安全研究院”等机构
行业研究	与行业龙头单位联合组建了“交通运输大数据系统与安全实验室”、“清洁能源大数据安全技术研究中心”、“智慧能源大数据安全研究中心”、“电力行业大数据安全研究中心”、“金融科技大数据安全研究中心”和“智造生活大数据安全研究中心”等研究机构

来源：公司招股说明书，国金证券研究所

- **科技成果与产业深度融合，转化率高。**2017-2019 年，公司主营业务除“硬件及其他”外，均为公司通过研发技术产业化、科技成果与产业深度融合的产品及服务产生的收入，即技术产业化形成的收入，占主营业务收入的比例分别为 97.33%、78.28%及 78.17%。公司核心技术产品为应用了公司 28 项核心技术的产品，2017-2019 年，核心技术产品收入占比分别为 77.04%，75.55%，77.57%。

图表 41：2017-2019 年奇安信技术产业化收入不断增加（单位：亿元）

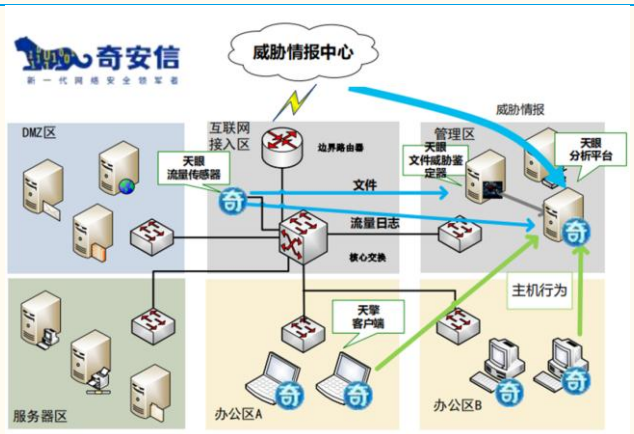


来源：公司招股说明书，国金证券研究所

3.2 威胁情报数据库拥有海量数据，助力主动防御业务

- **终端云端边界全布局，丰富数据助力主动防御业务。**随着网络安全行业从被动防御逐渐迈入主动防御阶段，现阶段的网络安全产品需要基于现状、基于所处的网络环境，对整体的安全态势进行评估，针对未来可能发生的威胁及安全风险进行预判和防御。2015 年公司发布“数据驱动安全”理念。公司通过在各行业客户端丰富的硬件基础安全产品的补齐，在云端汇集成自有的多维度海量安全数据，并以此为支撑利用大数据分析技术和威胁情报平台，围绕云端进行新型安全产品布局，帮助客户建立实现监测预警、威胁检测、溯源分析、响应处置等能力的主动积极防御体系。
- **安全大数据是整套体系性的核心支撑。**在整套体系中，最为核心的支撑就是安全大数据。如果整套体系缺少安全大数据的支撑，那么平台就无法有效比对和检测攻击信息，威胁感知系统（天眼）就因此变成摆设。而奇安信凭借在终端、网关、云端、NGSOC 等领域的高市占率，可以轻松挖掘到客户以往的被攻击行为数据、被攻击特征、恶意样板库等等，安全大数据得以不断汇集。此外，奇安信还拥有专门的大数据研发平台“诺亚”，专注安全大数据的挖掘搜集及分析处理，及时有效地解决发现的各类威胁。

图表 42：威胁感知系统（天眼）产品架构



来源：公司官网，国金证券研究所

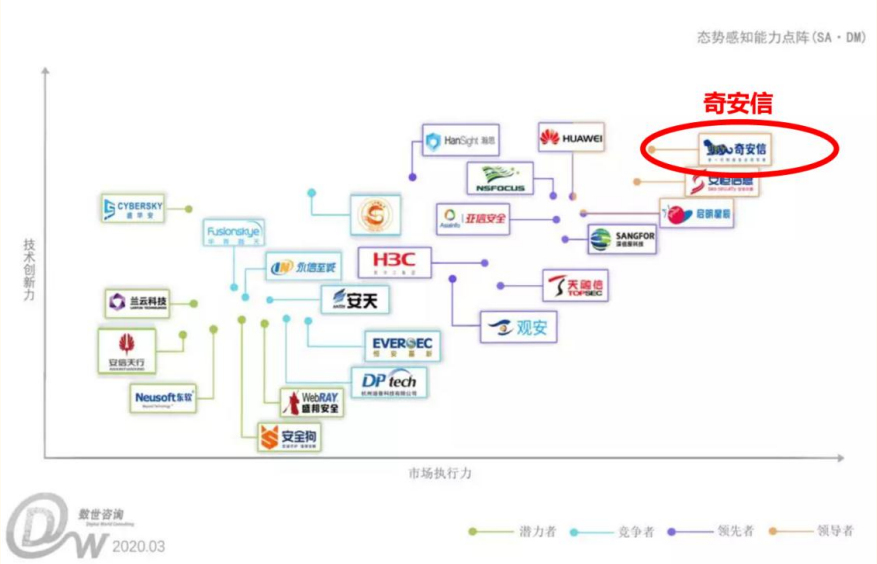
图表 43：威胁感知系统（天眼）产品四大能力



来源：公司官网，国金证券研究所

- **奇安信在态势感知领域处于绝对领导者地位。**在威胁情报数据库方面，奇安信是国内最大的威胁情报数据拥有者之一。同时，公司还拥有 IP、DNS、URL、文件黑白名单四大信誉数据库，满足海量数据需求。根据第三方调研机构数世咨询发布的 2019 年《网络安全态势感知能力指南》报告可以得知，无论是技术创新力还是市场执行力，奇安信都处于中国态势感知解决方案的绝对领导者地位。

图表 44：公司处于中国态势感知解决方案绝对领导者地位

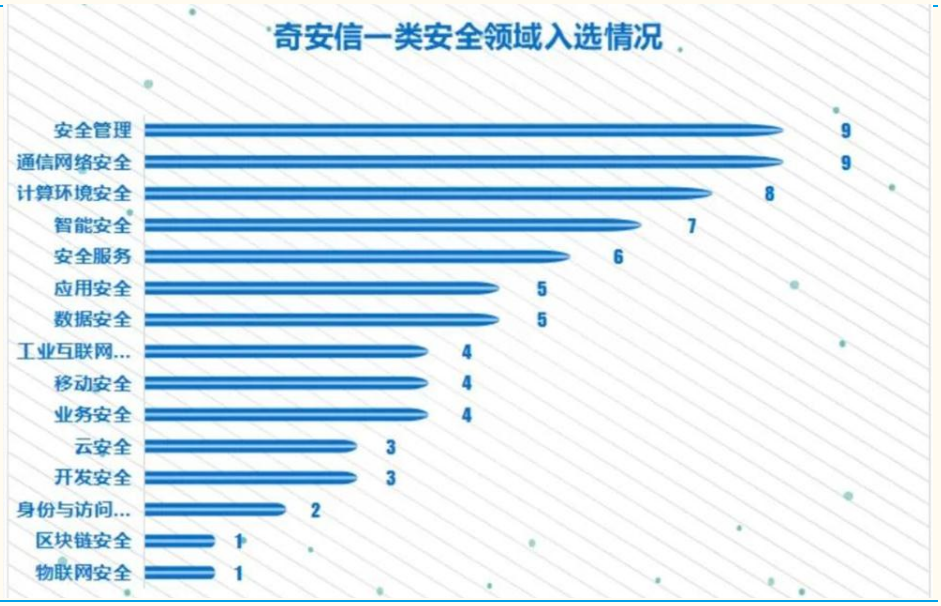


来源：数世咨询，国金证券研究所

3.3 产品线丰富，新安全业务布局最全面前瞻

- **产品覆盖多个领域，布局全面。**公司是全领域覆盖的综合型网络安全厂商，据 2020 年 3 月安全牛发布的第七版中国网络安全行业全景图显示，公司产品覆盖全部 15 类一级安全领域和 71 类二级细分领域，在 313 家国产网络安全企业和相关行业机构中，奇安信成为安全牛评选出的全景图细分领域最多的网络安全企业。

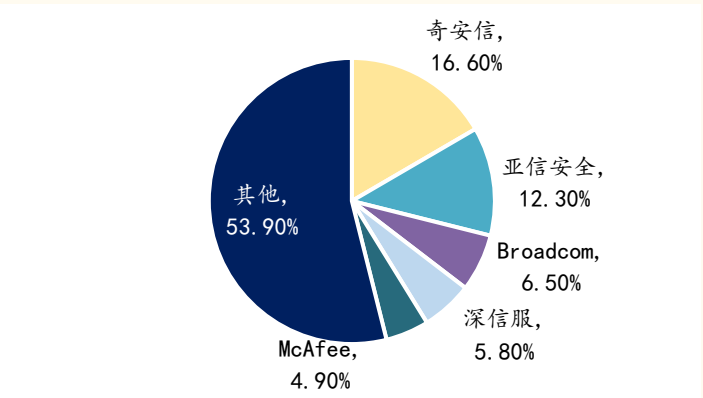
图表 45：公司在安全牛中国网络安全行业全景图中一类安全领域入选情况



来源：安全牛，公司官网，国金证券研究所

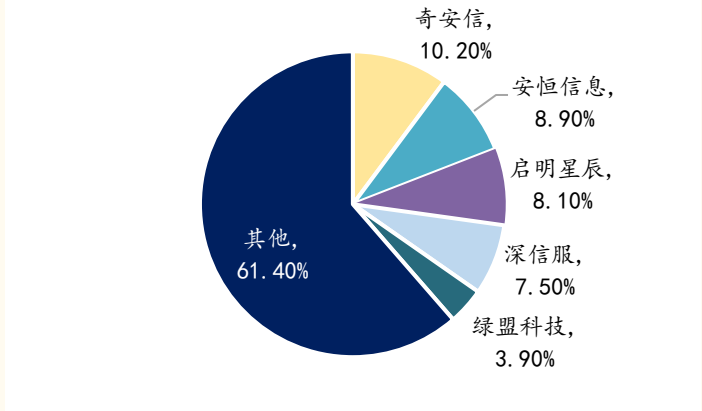
- **领跑中国网络安全市场，细分领域份额占比高。**赛迪咨询数据显示，奇安信在终端安全、安全服务、安全管理平台、云安全等细分领域均列国内第一：终端安全市场占比 20.5%，近日更独家中标中国联通终端安全管理项目（国内最大规模终端安全项目之一）；安全服务市场占比 6.3%；安全管理平台市场占比 23.9%；云安全市场占比 5.7%。此外，UTM 市场，奇安信以 17.3%的市场份额位居第三；Web 安全市场，以 21.0%市场占比位居第二。IDC 数据显示，奇安信在终端安全软件、安全分析与威胁情报、中国安全管理平台、2019 中国安全资源池市场占有率均第一。

图表 46：2020 年上半年终端安全软件市场



来源：IDC，国金证券研究所

图表 47：2020 年上半年中国安全分析和威胁情报市场



来源：IDC，国金证券研究所

■ **募投资金布局云、人、工、物、移等新安全赛道，加速新安全体系建设。**2020 年 7 月，公司科创板上市，募集资金共 57.19 亿元。扣除各项发行费用后，公司实际可使用募集资金为 53.96 亿元，募集资金将用于云和大数据安全防护与管理运营中心建设项目、物联网安全防护与管理系统项目、工业互联网安全服务中心建设项目、安全服务化建设项目、基于零信任的动态可信访问控制平台建设项目、网络空间测绘与安全态势感知平台建设项目，以及补充公司流动资金。云计算、大数据、物联网、工业互联网等新技术领域风口已至，公司通过将大量募集资金投入以上领域，构筑技术优势，进一步完善公司新赛道产品布局，以增强公司网络安全领域核心技术的竞争力，抢占新安全风口，深化公司内生安全及数据驱动安全战略，推动全时段、全方位的主动安全防御体系全面发展。

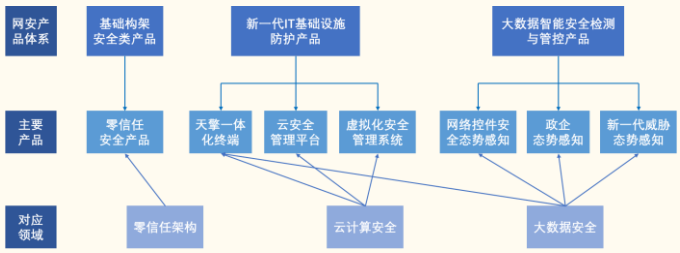
图表 48：募投资金加码新安全布局

序号	募集资金使用项目	项目投资总额（万元）	拟投入募集资金（万元）
1	云和大数据安全防护与管理运营中心建设项目	84,925.75	84,925.75
2	物联网安全防护与管理系统项目	58,423.67	58,423.67
3	工业互联网安全服务中心建设项目	69,548.73	69,548.73
4	安全服务化建设项目	95,323.24	95,323.24
5	基于“零信任”的动态可信访问控制平台建设项目	31,441.32	31,441.32
6	网络空间测绘与安全态势感知平台建设项目	67,976.39	67,976.39
7	补充流动资金	42,360.91	42,360.91
合计		450,000.00	450,000.00

来源：公司招股说明书，国金证券研究所

■ **公司新赛道产品全面布局。**现阶段公司核心产品主要聚焦网络安全领域的“新赛道”产品，新赛道包括 5G 引领下的三项新兴技术，即云计算安全领域、大数据安全领域、以及物联网、工业互联网安全领域。奇安信新一代 IT 基础设施防护产品和大数据智能安全检测与管控产品均包含对标以上新赛道的网安产品。

图表 49：奇安信安全产品体系及主要的新安全产品



来源：公司招股说明书，国金证券研究所

图表 50：新赛道产品对标新兴领域需求

	产品体系	主要产品	新兴领域
新赛道产品	基础架构安全产品	零信任身份安全产品	零信任基础架构
	新一代 IT 基础设施防护产品体系	天擎一体化终端	云计算与大数据安全防护领域
		云安全管理平台	云计算安全防护领域
		虚拟化安全管理系统	
	大数据智能安全检测与管控产品体系	网络控件安全态势感知	大数据安全防护领域
		政企态势感知与安全运营管理平台	
		新一代威胁态势感知	

来源：公司招股说明书，国金证券研究所

- **新安全产品收入占比不断提升。**目前，公司布局的新安全产品主要包括零信任身份安全、天擎一体化终端、云安全管理平台、虚拟化安全管理系统、网络控件安全态势感知、政企态势感知和新一代威胁态势感知等产品。2017-2019 年，新安全产品累计收入占比由 27.65%提升至 34.18%。

图表 51：2017-2019 年奇安信新安全产品收入占比不断提升（单位：亿元）

新安全产品	2017	2018	2019
零信任身份安全	0.00	0.00	0.13
天擎一体化终端	1.12	1.90	4.22
云安全管理平台	0.01	0.14	0.67
虚拟化安全管理系统	0.26	0.60	0.81
网络控件安全态势感知	0.46	0.67	1.50
政企态势感知	0.24	0.54	1.40
新一代威胁态势感知	0.18	0.57	2.05
合计	2.27	4.43	10.78
收入占比	**27.65%**	**24.37%**	**34.18%**

来源：公司招股说明书，国金证券研究所

3.4 政府资源丰富，国家队背景助力政企市场持续拓展

- **多次参与国家级重大网络安保活动。**公司自成立以来，多次参与到国家重大网络安全保护活动中。近年来，中国频繁开展两会、进博会、一带一路论坛、达沃斯论坛、抗疫网安等重大活动，公司连续多年配合各级省政府、公安部、网信部等国家级部门完成以上活动的网络安全防护保障工作，协助国家应对重大突发事件。2019 年 12 月，奇安信正式成为北京 2022 年冬奥会冬残奥会的官方网络安全服务及杀毒软件赞助商。此外，公司还多次支撑国家部门开展的网络攻防实战化演习，并取得优异的成绩，彰显了公司技术实力已获得国家和社会的高度认可。

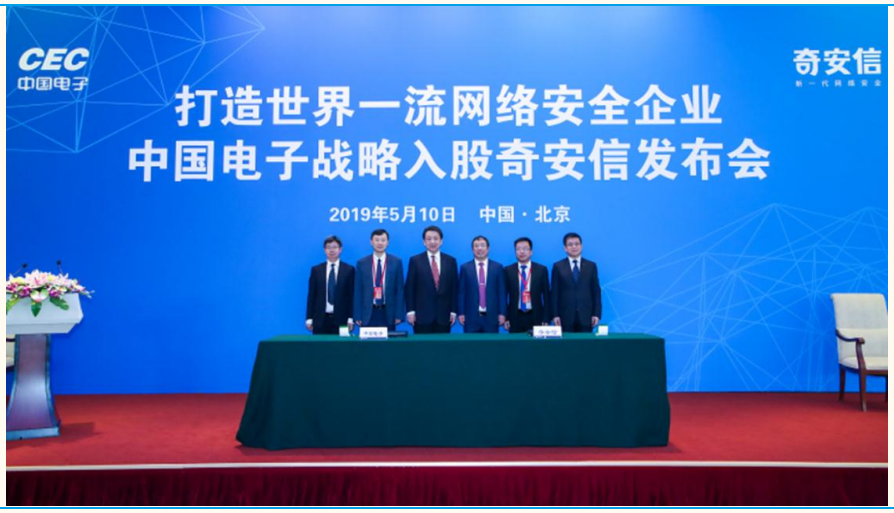
图表 52：2017-2020 年奇安信参与多项重大安保活动

时间	参与的重大网络安保活动
2017	十九大、全国两会、一带一路会议、达沃斯论坛、金砖国家峰会·厦门、国际刑警大会、晚直播、特朗普访华、国际财富论坛等
2018	全国两会、博鳌亚洲论坛、达沃斯论坛、俄罗斯世界杯直播、春晚直播、中非合作论坛改革开放40周年、中国进博会等
2019	全国两会、北京市两会、一带一路会议、博鳌论坛、夏季达沃斯论坛、亚洲文明对话大春晚直播、建国70周年活动、上海进博会、电商双十一等
2020	全国两会、火神山、雷神山等医院网络安全系统、顺义智能网联汽车示范区等

来源：公司官网，国金证券研究所

- 2019 年 5 月，中国电子通过旗下明洛投资 37.31 亿元战略入股奇安信，持有公司 17.95%的股份，代替三六零集团成为公司第二大股东，本次中国电子入股，为战略性投资，意味着奇安信正式成为网安国家队之一。

图表 53：2019 年 5 月 10 日，举行中国电子战略入股奇安信发布会



来源：公司微信公众号，国金证券研究所

- **PKS 自主可信生态体系成立**。2017 年，中国电子正式发布了由其主导构建的全新“自主可信”绿色开放 PK 生态体系。其中，P 代表天津飞腾（Phytium）兼容 ARM V8 指令集的处理器芯片，K 代表麒麟软件（Kylin）操作系统，二者深度适配。PK 体系拥有从操作系统、中间件、数据库、安全整机到应用系统的国内最完整的自主安全产业链，并可以应用于政务、金融、交通互联网等重要领域。同时，基于网络强国目标，面向全球开放合作，推动 ARM 架构在重要行业领域信息化和网络安全工作中的应用。
- **奇安信成功入局中电 PKS 生态体系**。奇安信作为目前国内规模最大的网络安全公司，在中国电子战略入股后，成功纳入到 PK2.0 生态体系中。双方将在技术创新、资源整合、重大项目建设等方面开展合作。通过与中国电子的战略合作，奇安信将自身强大的安全防护能力平移到自主可信的 PKS 底座上，实现深度融合，展现更强大的安全能力，共同打造国产化全链条解决方案。除此之外，网络安全作为机密、敏感行业，可以直接影响到国家及下属企业的安全和利益，因此只有融入国家背景，才能更好地实现安全服务。中国电子的重量级客户遍布政府、央企和各种机构，渠道丰富健全。奇安信此次成为中国电子的战略级合作伙伴，意味着奇安信可以借助中国电子强大的营销渠道和市场背景，用更低的成本、更快的速度横向、纵向拓展市场。

图表 54：飞腾携手麒麟软件打造 PKS 自主可信生态体系



来源：国金证券研究所制

四、盈利预测与投资建议

4.1 盈利预测

盈利预测假设及其必要的解释：

网络安全产品：网络安全产品是公司的主要业务，受益于大数据安全、云安全、物联网安全及工业互联网安全等新兴安全需求的旺盛，该项业务依旧处于高速增长的态势，但由于 20Q4 疫情反复导致部分订单收入确认延迟，造成 20 年增速有所放缓，但我们预计 21、22 年将会再次回升。因此，预计 20-22 年该业务营收同比增速分别为 27.36%、40.74%、39.36%。

网络安全服务业务：随着行业结构的变化，我国网络安全服务在整个网络安全市场中占比不断提升，安全服务需求不断增加，公司在安全服务投入力度不断加大，前三季度安全服务业务占比已超 15%。预计 20-22 年该业务保持快速增长，同比增速分别为 70%、70%、70%。

硬件及其他：硬件业务主要是采购第三方硬件及集成服务。预计 20-22 该业务营收保持平稳增长，同比增速分别为 30%、30%、30%。

其他业务：预计 20-22 年增速分别为 10%、20%、20%。

图表 55：公司分业务营收预测（单位：亿元）

单位：亿元	2018A	2019A	2020E	2021E	2022E
网络安全产品	11.85	20.95	26.68	37.55	52.33
YoY	76.60%	76.79%	27.36%	40.74%	39.36%
网络安全服务	2.20	3.67	6.24	10.61	18.03
YoY	96.43%	66.82%	70.00%	70.00%	70.00%
硬件及其他	3.90	6.87	8.93	11.61	15.09
YoY	1757.14%	76.15%	30.00%	30.00%	30.00%
其他业务	0.22	0.05	0.06	0.07	0.08
YoY	29.41%	-77.27%	10.00%	20.00%	20.00%
合计	18.17	31.54	41.91	59.83	85.53
YoY	121.32%	73.58%	32.87%	42.78%	42.95%

来源：Wind，国金证券研究所

毛利率假设：

网络安全产品，主要基于公司自研的网络安全产品，具有明显的市场竞争优势，毛利率较高，且保持稳定。**网络安全服务业务**，安全服务成本主要为直接人工支出及外包实施成本，预计该项毛利率持续保持平稳。**安全硬件及其他**，硬件及其他业务的成本主要来自公司在系统集成性质的网络安全项目中向第三方采购的硬件，由于第三方硬件的市场较为成熟、价格相对透明，因此硬件及其他业务毛利率相对较低。公司其他业务预计毛利率基本保持稳定。综上，预计 20-22 年公司毛利率分别为 57.03%、58.40%和 59.26%。

图表 56：公司分业务毛利率预测

	2018A	2019A	2020E	2021E	2022E
网络安全产品	72.48%	73.10%	73.40%	73.75%	73.79%
网络安全服务	57.06%	63.24%	64.00%	64.50%	64.00%
硬件及其他	1.36%	3.18%	3.00%	3.00%	3.00%
其他业务	100.00%	79.72%	95.00%	96.00%	96.00%
综合	55.68%	56.72%	57.03%	58.40%	59.26%

来源：Wind，国金证券研究所

费用率假设：

公司主营业务较为成熟，安全服务业务等发展空间广阔，但考虑公司推出多项新产品，需持续进行人员投入，预计费用率基本保持稳定。

综上，预计公司 20-22 年营收为 41.91 亿元、59.83 亿元和 85.53 亿元，净利润为-3.13、-1.16、1.56 亿元。

4.2 投资建议及估值

我们采用市销率法对奇安信进行估值：

我们通过观察海外高速发展期的网络安全相关的公司 Palo Alto、CrowdStrike、Palantir、Okta 等，发现在业务高速增长期，资本市场给予的平均 PS 倍数在 25 倍左右，与奇安信发展路径相似的 CrowdStrike 最高 PS 倍数甚至达到 60 倍，因此，我们给予公司 20-22 年 PS 倍数分别为 25/20/15 倍，对应 22 年目标市值 1283.02 亿元，对应目标价为 188.68 元，首次覆盖给予“买入”评级。

图表 57：PaloAlto 高速发展期的 PS(TTM)情况



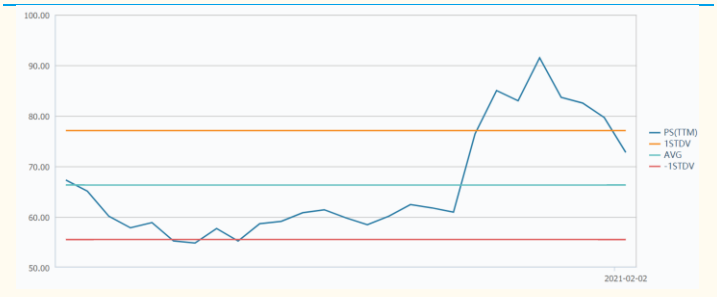
来源：wind，国金证券研究所

图表 58：CrowdStrike 高速发展期的 PS(TTM)情况



来源：wind，国金证券研究所

图表 59：Palantir 高速发展期的 PS(TTM)情况



来源：wind，国金证券研究所

图表 60：Okta 高速发展期的 PS(TTM)情况



来源：wind，国金证券研究所

五、风险提示

- **市场竞争加剧。**我国网络安全行业虽然处于高速发展期，但整体市场格局分散，新进者较多，而且随着国家网络安全战略确立，政企安全需求增加，以及科创板和注册制的推行，网安行业优质公司也越来越多，从而导致行业竞争也日益加剧。
- **网络安全政策推进不及预期。**国家颁布多个网络安全相关政策，存在政策推进及落地不及预期的风险。
- **商誉减值风险。**截至到 20Q3 公司商誉账面价值为 12.21 亿元，主要是收购网神等企业，存在业绩不达预期，导致商誉减值的风险。
- **限售股解禁风险。**公司将于 2021 年 7 月 22 日，解禁 38,292.38 万股，为首发原股东限售股，解禁数量巨大，占解禁前流通股的 523.37%，存在对公司股价造成冲击的风险。

单击或点击此处输入文字。

附录：三张报表预测摘要

损益表（人民币百万元）

	2017	2018	2019	2020E	2021E	2022E
主营业务收入	**821**	**1,817**	**3,154**	**4,191**	**5,983**	**8,553**
增长率		121.2%	73.6%	32.9%	42.8%	43.0%
主营业务成本	-206	-805	-1,365	-1,801	-2,489	-3,485
%销售收入	25.1%	44.3%	43.3%	43.0%	41.6%	40.7%
毛利	615	1,012	1,789	2,390	3,495	5,068
%销售收入	74.9%	55.7%	56.7%	57.0%	58.4%	59.3%
营业税金及附加	-30	-36	-33	-42	-60	-86
%销售收入	3.6%	2.0%	1.0%	1.0%	1.0%	1.0%
销售费用	-431	-800	-1,118	-1,359	-1,828	-2,462
%销售收入	52.5%	44.0%	35.4%	32.4%	30.6%	28.8%
管理费用	-232	-332	-470	-541	-688	-855
%销售收入	28.3%	18.3%	14.9%	12.9%	11.5%	10.0%
研发费用	-541	-818	-1,047	-1,299	-1,616	-2,282
%销售收入	65.9%	45.0%	33.2%	31.0%	27.0%	26.7%
息税前利润（EBIT）	-619	-975	-879	-852	-697	-616
%销售收入	n.a	n.a	n.a	n.a	n.a	n.a
财务费用	37	-30	-22	53	61	29
%销售收入	-4.5%	1.7%	0.7%	-1.3%	-1.0%	-0.3%
资产减值损失	-213	-202	-74	-7	-10	-7
公允价值变动收益	0	0	0	0	0	0
投资收益	-6	77	196	200	300	400
%税前利润	n.a	-8.1%	-36.4%	-56.5%	-237.7%	194.2%
营业利润	-706	-953	-536	-354	-126	206
营业利润率	n.a	n.a	n.a	n.a	n.a	2.4%
营业外收支	2	0	-3	0	0	0
税前利润	-703	-953	-539	-354	-126	206
利润率	n.a	n.a	n.a	n.a	n.a	2.4%
所得税	1	0	-14	0	0	0
所得税率	n.a	n.a	n.a	n.a	n.a	0.1%
净利润	-702	-953	-553	-353	-126	206
少数股东损益	-72	-81	-58	-40	-10	50
归属于母公司的净利润	**-630**	**-872**	**-495**	**-313**	**-116**	**156**
净利率	n.a	n.a	n.a	n.a	n.a	1.8%

现金流量表（人民币百万元）

	2017	2018	2019	2020E	2021E	2022E
净利润	-702	-953	-553	-353	-126	206
少数股东损益	-72	-81	-58	-40	-10	50
非现金支出	272	287	144	40	43	35
非经营收益	-20	-32	-166	-208	-300	-400
营运资金变动	-66	-259	-609	-1,156	-609	-338
经营活动现金净流	**-516**	**-956**	**-1,184**	**-1,678**	**-992**	**-497**
资本开支	-63	-100	-283	-1,247	-1,030	-930
投资	-505	-26	-624	-200	-150	-100
其他	175	-29	687	200	300	400
投资活动现金净流	**-393**	**-154**	**-219**	**-1,247**	**-880**	**-630**
股权募资	2,112	2,150	1,506	5,635	0	0
债权募资	0	0	-323	-100	0	0
其他	-630	-266	-255	0	0	-62
筹资活动现金净流	**1,481**	**1,884**	**927**	**5,535**	**0**	**-62**
现金净流量	**572**	**774**	**-477**	**2,611**	**-1,872**	**-1,190**

资产负债表（人民币百万元）

	2017	2018	2019	2020E	2021E	2022E
货币资金	861	1,646	1,258	3,869	1,997	807
应收款项	1,173	1,556	1,674	2,030	2,823	3,786
存货	449	611	749	822	1,191	1,574
其他流动资产	112	179	307	1,072	1,287	1,329
流动资产	2,595	3,991	3,989	7,793	7,297	7,497
%总资产	49.2%	58.8%	55.7%	62.9%	55.9%	52.6%
长期投资	443	554	509	709	859	959
固定资产	57	949	1,190	2,490	3,490	4,390
%总资产	1.1%	14.0%	16.6%	20.1%	26.8%	30.8%
无形资产	1,292	1,228	1,370	1,392	1,399	1,405
非流动资产	2,681	2,791	3,166	4,592	5,748	6,755
%总资产	50.8%	41.2%	44.3%	37.1%	44.1%	47.4%
资产总计	**5,275**	**6,782**	**7,155**	**12,384**	**13,046**	**14,252**
短期借款	0	0	0	0	0	0
应付款项	1,444	1,802	1,306	1,140	1,561	2,176
其他流动负债	479	594	662	880	1,229	1,651
流动负债	1,923	2,396	1,968	2,021	2,790	3,827
长期贷款	0	0	0	0	0	0
其他长期负债	59	109	146	42	60	86
负债	1,982	2,504	2,114	2,063	2,850	3,913
普通股股东权益	3,251	4,297	5,022	10,344	10,228	10,321
其中：股本	22	149	578	680	680	680
未分配利润	-798	-1,669	-2,164	-2,478	-2,594	-2,501
少数股东权益	43	-19	18	-22	-32	18
负债股东权益合计	**5,275**	**6,782**	**7,155**	**12,384**	**13,046**	**14,252**

比率分析

	2017	2018	2019	2020E	2021E	2022E
每股指标						
每股收益	N/A	N/A	-0.857	-0.461	-0.171	0.229
每股净资产	N/A	N/A	8.694	15.220	15.049	15.187
每股经营现金净流	-0.194	-0.203	-2.050	-2.468	-1.459	-0.732
每股股利	0.000	0.000	0.000	0.000	0.000	0.092
回报率						
净资产收益率	-19.38%	-20.29%	-9.85%	-3.03%	-1.13%	1.51%
总资产收益率	-11.94%	-12.85%	-6.92%	-2.53%	-0.89%	1.09%
投入资本收益率	-18.73%	-22.74%	-17.87%	-8.25%	-6.83%	-5.95%
增长率						
主营业务收入增长率	N/A	121.22%	73.61%	32.86%	42.78%	42.95%
EBIT增长率	N/A	57.48%	-9.85%	-3.02%	-18.22%	-11.57%
净利润增长率	N/A	38.41%	-43.22%	-36.67%	-62.97%	N/A
总资产增长率	N/A	28.56%	5.49%	73.09%	5.34%	9.24%
资产管理能力						
应收账款周转天数	50.0	77.1	106.5	145.0	140.0	129.0
存货周转天数	397.9	240.2	181.8	170.0	180.0	170.0
应付账款周转天数	266.5	191.4	187.9	180.0	180.0	180.0
固定资产周转天数	25.4	20.0	22.6	121.5	115.6	106.5
偿债能力						
净负债/股东权益	-26.14%	-38.48%	-24.96%	-37.48%	-19.59%	-7.81%
EBIT利息保障倍数	16.7	-32.2	-39.6	16.1	11.5	21.2
资产负债率	37.57%	36.93%	29.55%	16.65%	21.85%	27.45%

来源：公司年报、国金证券研究所

市场中相关报告评级比率分析

日期	一周内	一月内	二月内	三月内	六月内
买入	6	29	39	47	69
增持	0	0	0	2	0
中性	0	0	0	0	0
减持	0	0	0	0	0
评分	**1.00**	**1.00**	**1.00**	**1.04**	**1.00**

来源：朝阳永续

市场中相关报告评级比率分析说明：

市场中相关报告投资建议为“买入”得 1 分，为“增持”得 2 分，为“中性”得 3 分，为“减持”得 4 分，之后平均计算得出最终评分，作为市场平均投资建议的参考。

最终评分与平均投资建议对照：

1.00 =买入； 1.01~2.0=增持 ； 2.01~3.0=中性
3.01~4.0=减持

投资评级的说明：

买入：预期未来 6—12 个月内上涨幅度在 15%以上；
增持：预期未来 6—12 个月内上涨幅度在 5%—15%；
中性：预期未来 6—12 个月内变动幅度在 -5%—5%；
减持：预期未来 6—12 个月内下跌幅度在 5%以上。

特别声明：

国金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。

本报告版权归“国金证券股份有限公司”（以下简称“国金证券”）所有，未经事先书面授权，任何机构和个人均不得以任何方式对本报告的任何部分制作任何形式的复制、转发、转载、引用、修改、仿制、刊发，或以任何侵犯本公司版权的其他方式使用。经过书面授权的引用、刊发，需注明出处为“国金证券股份有限公司”，且不得对本报告进行任何有悖原意的删节和修改。

本报告的产生基于国金证券及其研究人员认为可信的公开资料或实地调研资料，但国金证券及其研究人员对这些信息的准确性和完整性不作任何保证，对由于该等问题产生的一切责任，国金证券不作出任何担保。且本报告中的资料、意见、预测均反映报告初次公开发布时的判断，在不作事先通知的情况下，可能会随时调整。

本报告中的信息、意见等均仅供参考，不作为或被视为出售及购买证券或其他投资标的邀请或要约。客户应当考虑到国金证券存在可能影响本报告客观性的利益冲突，而不应视本报告为作出投资决策的唯一因素。证券研究报告是用于服务具备专业知识的投资者和投资顾问的专业产品，使用时必须经专业人士进行解读。国金证券建议获取报告人员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。报告本身、报告中的信息或所表达意见也不构成投资、法律、会计或税务的最终操作建议，国金证券不就报告中的内容对最终操作建议做出任何担保，在任何时候均不构成对任何人的个人推荐。

在法律允许的情况下，国金证券的关联机构可能会持有报告中涉及的公司所发行的证券并进行交易，并可能为这些公司正在提供或争取提供多种金融服务。

本报告反映编写分析员的不同设想、见解及分析方法，故本报告所载观点可能与其他类似研究报告的观点及市场实际情况不一致，且收件人亦不会因为收到本报告而成为国金证券的客户。

根据《证券期货投资者适当性管理办法》，本报告仅供国金证券股份有限公司客户中风险评级高于 C3 级（含 C3 级）的投资者使用；非国金证券 C3 级以上（含 C3 级）的投资者擅自使用国金证券研究报告进行投资，遭受任何损失，国金证券不承担相关法律责任。

此报告仅限于中国大陆使用。

上海

电话：021-60753903

传真：021-61038200

邮箱：researchsh@gjzq.com.cn

邮编：201204

地址：上海浦东新区芳甸路 1088 号紫竹国际大厦 7 楼

北京

电话：010-66216979

传真：010-66216793

邮箱：researchbj@gjzq.com.cn

邮编：100053

地址：中国北京西城区长椿街 3 号 4 层

深圳

电话：0755-83831378

传真：0755-83830558

邮箱：researchsz@gjzq.com.cn

邮编：518000

地址：中国深圳市福田区中心四路 1-1 号嘉里建设广场 T3-2402