网络安全产业链梳理　行业增长逻辑究竟是什么?

我们今天研究的这个赛道，极其特殊，几乎所有的信息产业发展，都离不开它的“保驾护航”。这个赛道的龙头 A，业绩非常亮眼，2019 年营业收入增速 43%，2018 年 5 月上市以来，从 47.5 元，上升至峰值的 254 元，涨幅超过 430%。



图：龙头 A 走势

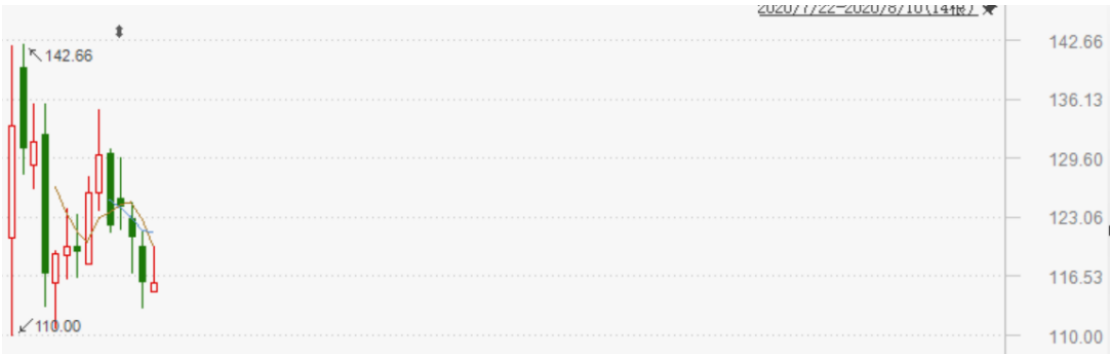
来源：wind

这个赛道的龙头 B，2019 年营业收入增速 22.5%，从 2018 年 11 月的低点 15 元，上涨至峰值高点的 31 元，涨幅超过 106%。



图：龙头 B 走势

来源：wind



图：龙头 C 走势，来源：东方财富 Choice 数据

上面的两家龙头 A、B，分别是**深信服**和**启明星辰**。而公司 C，则是刚刚登陆科创板的另外一家龙头——**奇安信**，其增长更为迅猛：2019 年同比增速 73%，过去三年复合增速 94%。

今天，我们要研究的产业链就是：**网络安全产业链。**

对于这个产业链，几个需要我们解决的问题是：

一是，网络安全，究竟解决的是客户的什么需求？其增长的逻辑是什么？

二是，这个市场的参与者增长情况如何？各自的竞争优势在哪里？

三是，目前阶段回报水平怎么样？后续是否还有提升空间？

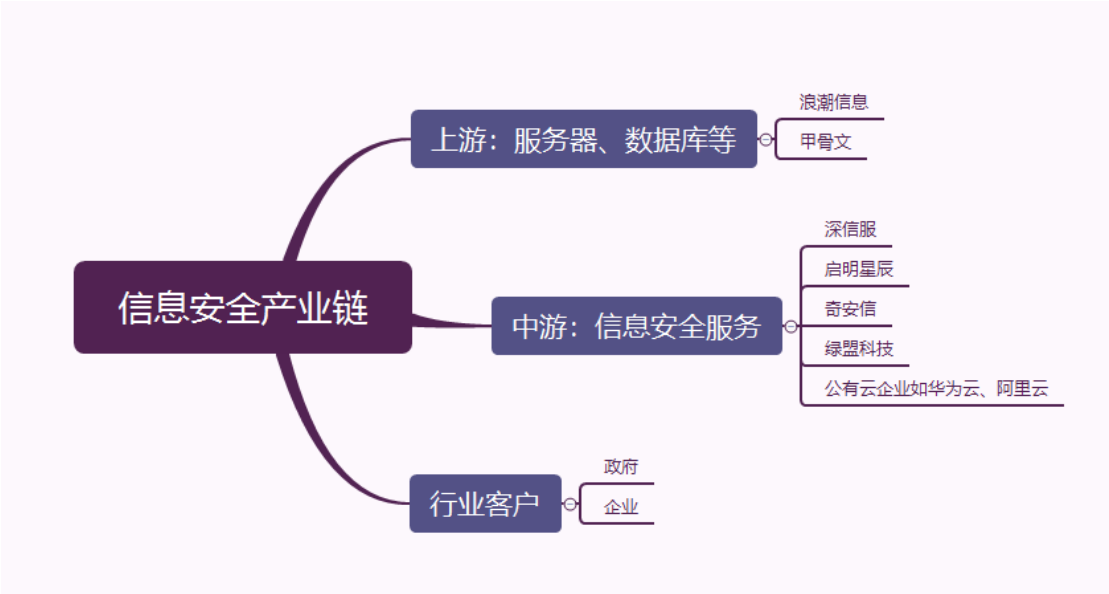
(壹)

网络安全产业链，从上游到下游，依次为：

上游——服务器、工控机、数据库、操作系统供应商，代表公司包括浪潮信息、Oracle 等。

中游——网络安全厂商，代表公司为**深信服、启明星辰、奇安信、绿盟科技**等。此外，我国部分公有云厂商也涉及安全业务，比如华为云、阿里云等。

下游——为政府、企业客户。其中，政府客户包括各级行政单位、公检法机关、卫生服务、教育机构、军队等；企业客户主要包括各类大、中型企业，比如电信、银行、地产集团、能源公司、大型零售企业等。



图：网络安全产业链

来源：塔坚研究

该产业链上游芯片、服务器应用范围较广，除了信息安全软件场景之外，还广泛应用于云计算、消费电子等诸多领域，各自的驱动力有所差异。而下游客户，主要包括政府和大型企业，各领域的经营模式、行业逻辑差异较大。因此，在本篇报告中，我们重点研究产业链中游的网络安全企业。

(贰)

网络安全产业，是指提供保障网络空间可靠性、安全性的产品和服务。传统的网络安全产品形态，主要包括防火墙、防病毒产品等。不过，随着信息技术和数字经济的迅猛发展，云计算、移动互联网的出现，使网络的边界越来越模糊，虚拟空间和实体空间结合的越来越紧密，网络安全形势也更加复杂化。因此，对于网络安全产品的需求也随之上升。



图：网络信息安全的需求

来源：华西证券

网络信息安全业务，包括：硬件、软件、服务三大类。其中：

硬件——强调特定“功能”属性，包括 VPN/防火墙、身份认证和鉴定，令牌/智能卡、入侵检测与防御、统一威胁管理等；

软件——强调对于系统的“管理”属性，包括身份管理，事件/漏洞管理，政策合规管理、终端/邮件/网站安全管理、威胁管理等；

服务——强调对于客户的“服务”属性，包括安全系统的咨询、项目实施、运维与相关技术培训。



图：网络信息安全产品分类

来源：华泰证券研究所

目前，我国的网络信息安全业务以硬件为主，而 USA 则以软件和服务为主。这主要由于，历史上我国网络安全支出以合规需求驱动，而在政府和大企业的预算体制下，安全硬件产品容易核算，从而导致我国网络安全支出硬件占比较高，软件占比少。

未来，随着网络边界的扩张及模糊化，以及企业安全防护意识的提升，未来，我国的软件和服务业务占比将随之提升。

综合来看，网络信息安全产业增长的驱动力，可以拆分为两部分：

1）随着信息化、数字化世界的扩张，带来的 **IT 支出增加**；

2）随着信息、网络空间中的安全需求的重要程度提升，带来的**网络安全开支渗透率提升。**

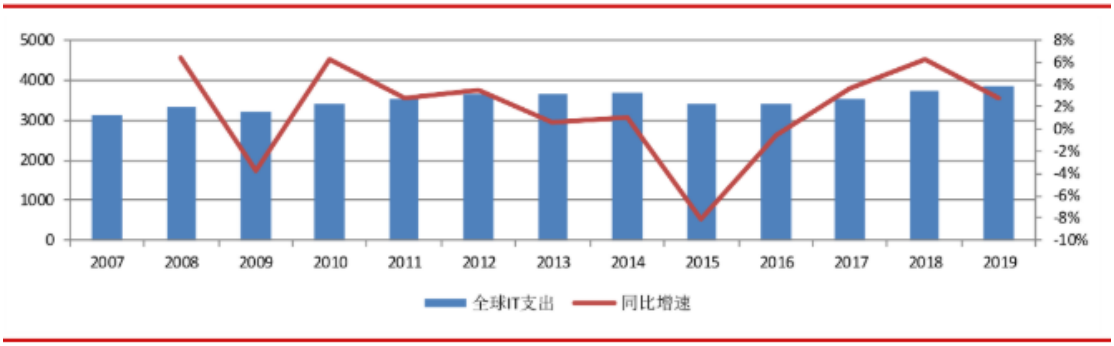
因此，网络信息安全市场规模的增速可以表示为：*信息安全市场规模增长=IT 支出增速*信息安全渗透率增速。*

（叁）

我们先来看全球 IT 支出增速：

IT 支出，是指为了搭建整个数字世界所进行的投入，其目的在于提升人类社会的生产和服务效率。

2019 年，全球 IT 支出为 3.74 万亿美元（折合人民币 26.1 万亿元），同比增长 0.5%。2007 年以来，全球 IT 支出呈现出波浪式增长的态势，近 13 年复合增速约为 1.93%。2019 年，中国 IT 支出为 4098 亿美元（2.8 万亿人民币），同比增长 4.48%。



图：全球 IT 支出　来源：wind

从长期来看，只要人类提升生产效率的追求不停息，数字世界的扩张就将持续。因此，IT 支出和全球数据增长、数字经济的扩张呈正相关关系。

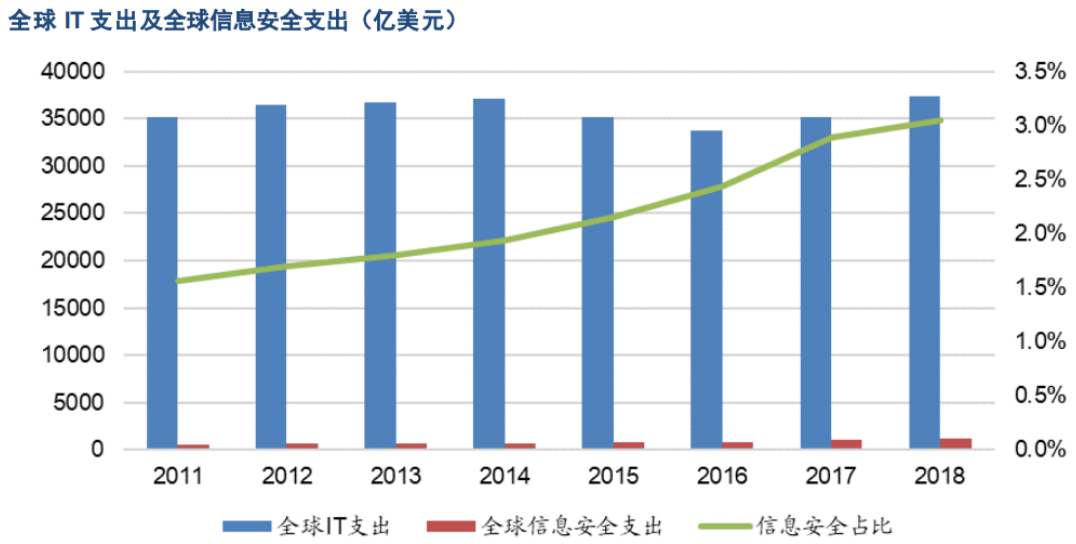
根据 Gartner 预测，2020 年全球 IT 支出将达到 3.9 亿美元（折合人民币约 27 万亿元），同比上升 3%。预计 2021 年将突破 4 万亿美元大关。鉴于我国数字经济的高速发展，我国 IT 支出将保持较高水平，此处我们保守假设我国 IT 支出增速和全球保持同步水平。

（肆）

再来看信息安全渗透率：

2011 年以来，全球网络安全渗透率持续上升，从 2011 年的不足 1.5%提升至 2018 年的 **3%**，七年复合增速高达 12%。

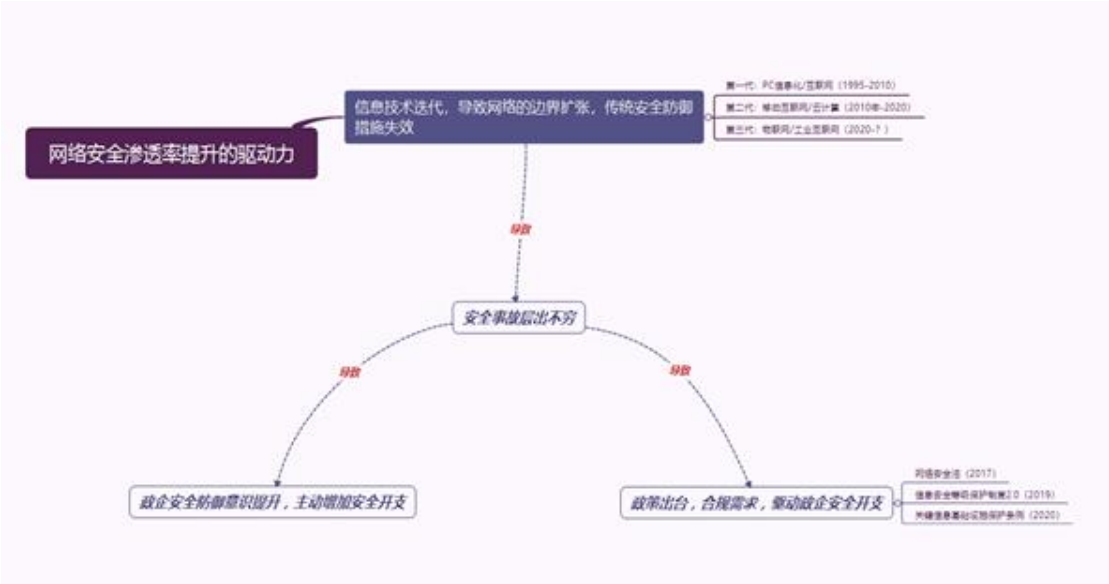
2018 年同时期，USA 的网络安全渗透率已经超过 10%。与此对应的，是我国网络安全渗透率仅为 1.7%，可以看出，我国与 USA 及全球平均水平的差距均较大。



图：网络信息安全市场渗透率

来源：东兴证券

那么，未来我国网络安全的渗透率是否会进一步提升？我们从以下几方面来看：



图：网络安全渗透率提升的驱动力

来源：塔坚研究

首先，是技术升级，带来了巨大的安全风险敞口。

通信和互联网技术的发展，让网络的边界持续扩张，数字空间和物理空间结合的越来越紧密，网络安全形势也逐级放大、更加复杂化。

第一级：前 3G 和 PC 互联网时代——仅实现了机器与机器之间的连接，数据和信息互联互通的维度是单一的。网络空间威胁所造成损失体现为信息泄露、系统瘫痪等少数场景。因此，网络安全需求仅体现在身份认证、防诈骗、防火墙、杀毒软件等少数场景。

第二级：3G、4G 和移动互联网时代——智能手机作为新的数据入口迅速普及，通信和互联网络实现了人与人的连接，而云计算让网络所承载的内容再次升级。随之而来的，是数据和信息互联的维度大幅度提升，个人、企业、政府等实体的位置、社交关系、财产、行为特征等数据全部进入了网络空间，网络空间威胁所造成的损失迅速放大。

第三级：5G、物联网、人工智能时代——网络的边界将继续大范围扩张，虚拟数字空间和物理实体世界将进一步无缝融合，网络空间威胁对社会造成的损害将进一步放大。

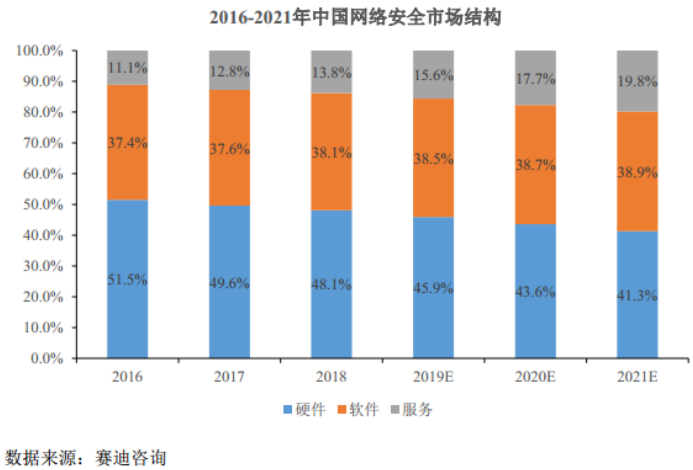
其次，技术升级带来的巨大的网络风险敞口，带来了越来越多的网络安全事故发生。

自 2015 年以来，全球范围内发生的网络安全事故数量激增。2018 年，数据泄露事件数量达 45 亿件，同比增长 133%。

据 CNCERT 发布的《2018 年中国互联网网络安全报告》披露，2018 年国家计算机网络应急中心协调处置网络安全事件约 10.6 万起，其中，网页仿冒、安全漏洞、恶意程序、网页篡改等安全事件较多。

随着重大安全事故的发生，一方面，有助于提升政府和企业购买安全服务的意愿，从而提升其对网络信息安全的支出；另一方面，重大安全事故，会促使政府出台相关政策，使得政企在合规需求的驱动下，提升网络安全开支。

此外，短期看，政策导向和合规需求，有助于促使安全软件和服务规模提升。我国网络安全市场中占比较高的子版块是硬件(41.3%)，其次为软件和服务，占比分别为 38.9%、19.8%。而对比全球市场来看，则以提供服务（64.4%）为主，其次是软件（26.2%）市场。



图：全球网络信息安全市场产品结构　来源：奇安信招股书

而近年来，随着网络攻击的增加，企业开始把网络安全视为一项重要的商业风险，并且更看重网络安全服务的持续性。因此，软件和服务支出合计占我国网络安全市场的比重逐年上升，从 2016 年的 48.5%上升至 2018 年的 58.7%。

鉴于安全服务和软件，是网络安全行业的主流形态，随着主动防御意识的提升，我国安全软件和服务领域可提升空间较大，有利于整个信息安全服务市场渗透率的进一步提升。

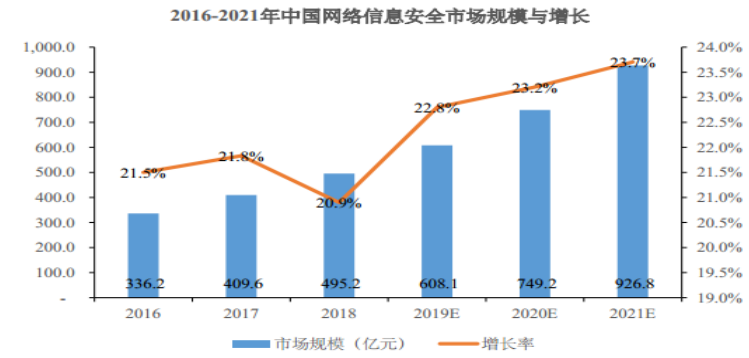
综上，我们假设未来 10 年，我国网络安全渗透率提升至 USA2018 年的水平（10%），由此推算出年复合增速保持 19%。

（伍）

对于网络信息安全产业链，后续跟踪时，我们需要重点关注以下几个行业高频数据：

1）网络安全支出：

2018 年，我国网络安全市场规模为 **495 亿元**，2019 年超过 **600 亿元**，预计 2021 年市场规模将达到 **926.8 亿元**，同比上涨 23.7%。2019-2021 年，复合增长率维持 **23%**。



图：信息安全市场增长情况

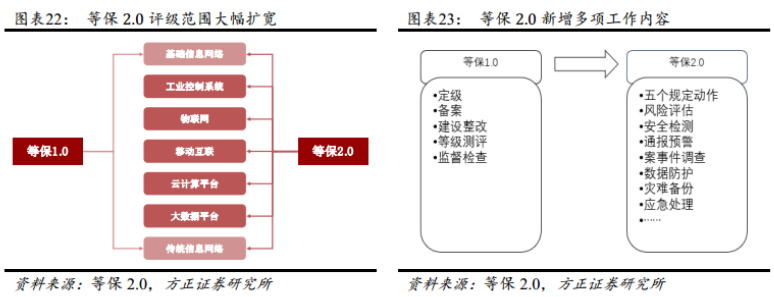
来源：奇安信招股书

2）网络安全相关法规、政策：

网络安全相关法律、法规的推出，将刺激政府和企业进行网络安全产品和服务的采购。其中，2019 年，由公安部颁布的《网路安全等级保护基本要求》（被称为等保 2.0 版本），对网络安全领域的合规标准做了升级。此次升级主要体现在两方面：

一是，在评级对象上，除了现有的信息系统，将工业控制系统、云计算、大数据、物联网等新兴技术应用纳入到了等级保护的评级范围；

二是，在工作内容上，传统的等级保护仅包括定级、备案、建设整改、等级测评和监督检查五大动作，而等保 2.0 新增了风险评估、安全检测、通报预警、案事件调查等方面的工作内容，等级保护的工作内容明显增多。



图：网络安全相关法规

来源：华泰证券研究所

（陆）

宏观和行业情况看完后，我们再来看看该领域的竞争格局，根据赛迪咨询数据，2019 年我国网络信息安全行业 CR4 市场占有率约为 **25%**，单一厂商的市场份额不超过 **10%**，竞争格局较为分散。其中，奇安信为该领域龙头，市占率为 5.2%，其次为启明星辰，市占率约为 5%。

我们主要从技术投入、渠道、业务规模三大维度，分别来看：

1）技术投入

技术投入是保证产品领先优势的基础，当下各家厂商都在布局前沿赛道，包括大数据安全、云计算安全、物联网安全、工业互联网安全、人工智能分析等。

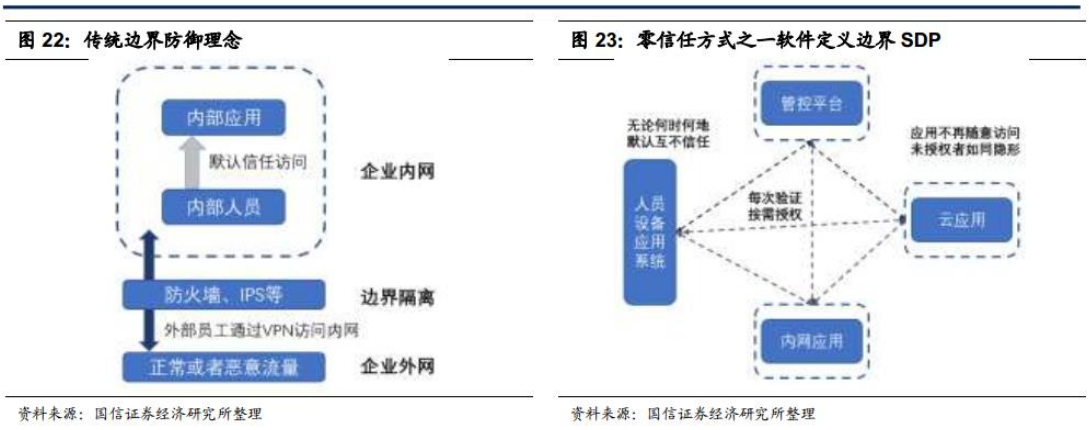
从研发费用率角度来看，奇安信遥遥领先，2019 年研发费用率为 33.2%，其他三家厂商差异不大，深信服(24.86%)、绿盟科技(20%)和启明星辰(19.5%)。

受益于高研发投入，奇安信在信息安全的前沿领域已取得初步成果：

A）零信任

随着云计算的兴起，部分应用被搬到云上，原本通过防火墙铸造的安全边界被打破，黑客可以通过多种手段渗透到企业内部的设备。“无边界”时代迫切需要新的保护方法，零信任概念应运而生（由 Forrester 分析师提出）。

其核心思想是：默认情况下，不应该信任网络内部和外部的任何人、设备、系统，需要基于认证和授权重构访问控制的信任基础，从而实现业务流程的安全可控。



图：零信任

来源：国信证券

2019 年，奇安信率先发布了“零信任安全参考架构 V1.0”和“零信任安全访问平台解决方案”，覆盖了政企行业用户的典型应用场景，并于 2019 年实现

1253.55 万元的收入。另外，奇安信集团的张泽洲荣获国内首位 Forrester 评选的零信任战略专家认证。

深信服、启明星辰、绿盟科技对零信任也均有相关投入。不过，截至 2019 年，均未披露具体成果。

B）态势感知

态势感知则是以数据驱动，在企业 IT 系统中布置探针设备，汇聚已有的和新增的各种安全设备的日志信息、攻击信息等。通过大数据和 AI 分析，对当前网络安全态势进行分析和判断，并通过可视化的方式进行展示和预警。实现了从传统被动安全防御的方式，变革为主动的、可视化的安全，属于当前安全服务的前沿领域。

而奇安信，是较早推动态势感知发展的厂商之一。2014 年开始，其提出了“数据驱动安全”的技术理念，着手采用大数据技术针对攻击行为进行检测和响应。当前，奇安信已经为监管部门建立了近百套真正大数据体系的态势感知平台，监管了上万家单位的关键信息基础设施。据统计，国内 85%以上的千万级态势感知项目均由奇安信建设和运营。

综上，从技术投入的角度看，奇安信通过较高的研发投入，在各前沿技术上均有一定成就，较其他公司存在一定优势。

2）渠道

由于网络安全产品和服务定制化属性较强，客户一旦选择某个安全产品或服务，则具有一定的迁移成本。因此，在产品和服务质量相差不大的前提下，对于网络安全公司来说，渠道覆盖和客户开发能力尤为重要，直接关系到收入规模的增速。

从渠道上来看，不同的下游客户，需要不同销售渠道。政府部门和大企业，需要直销开拓和维护，而中小型公司则需要经销渠道拓展。

而随着物联网技术带来的网络边界继续扩张，中小企业的安全需求将持续增长，是未来主要的增量市场。而较大的经销渠道占比，则有利于快速拓展中小企业客户。

因此，未来该领域的渠道优势，主要体现为**经销占比。**

对比来看，奇安信近年来逐渐拓展经销商渠道，2019 年为 68.54%（过去三年一直保持 50%以上）。其次，是深信服（经销占比为 22%）；绿盟科技从 2019 年开始显著加大经销渠道建设，效果还有待观察；而启明星辰，则仍以直销为主。

从销售费用率的角度看，除了启明星辰（22.5%）较低之外，各家相差不大，奇安信（35.44%）、深信服（35%）、绿盟科技（35.66%）。

综上，从渠道及客户开发能力的角度看，奇安信市场化布局较早，未来将更加受益于网络边界的持续扩张所带来的小公司安全需求增加。

3）业务规模

网络信息安全市场属于 B 端服务，需要长期的经验积累，行业壁垒较高，新进入者从零开始发展需要较长时间。因此，网络安全相关收入规模，代表了企业在当下产品的竞争力，是未来进行业务扩张的基础。

从这个角度来看，2019 年，启明星辰（30.89 亿元）和奇安信（31.54 亿元），收入规模较大。深信服其次，网络安全相关业务收入 27 亿元，绿盟科技为 16.7 亿元。

不过，需要注意的是，目前阿里云、腾讯云、华为云均涉足安全服务。由于未来中小企业的云服务将大概率依托公有云渠道分发（比如 USA 的 CrowdStrike 依托亚马逊 AWS 进行渠道分发），公有云厂商自身的安全业务，将对现有的纯安全厂商构成一定威胁。

我们来简单总结一下几家龙头公司的情况：

奇安信：无论在技术布局、渠道、收入规模上，均优于同行业其他公司。未来，其市占率进一步提升的空间较大。

深信服：在研发和销售渠道拓展上仅次于奇安信。*值得注意的是，深信服并不是一家纯粹的安全公司，安全业务仅占其收入规模的 62%，另外 38%包括私有云的融合计算和企业级无线服务（值得注意的是，深信服的融合计算业务属于目前 A 股市场的稀缺标的，市占率第三，排名前二的是华为和新华三）。*

启明星辰：在研发和销售渠道拓展方面较为保守。

绿盟科技：正在经历经销渠道的拓展阶段，未来拓展效果还无法确定。

综上，受益于研发投入较高、销售渠道布局较好，未来奇安信的市占率提升空间较大。

(柒)

好，行业增长驱动力看完后，我们再继续深入，梳理一下这条产业链图谱。

……

【参考资料如下，特此鸣谢】

[1]新时代证券：特高压重启在即，设备龙头投资机会显现，2019-01-28；[2]南方周末：京沪高铁启动上市，高铁究竟赚不赚钱？2019-02-27；

以上，为本行业报告部分内容。近期我们新开辟了基金笔记、宏观笔记、产业链梳理笔记三个研究系列。如需获取全部行业笔记、基金笔记、宏观笔记、建模笔记，请扫描下方二维码订阅专业版报告库。一分耕耘一分收获，只有厚积薄发的硬核分析，才能在关键时刻洞见未来。



扫码阅读优塾核心产品

专业版估值研报库

如需了解更多，请添加工作人员微信：ys_dsj

【版权与免责声明】1）关于版权：版权所有，违者必究，未经许可，不得以任何形式进行翻版、拷贝、复制。2）关于内容：我们只负责财务分析、产业研究，内容观点仅供参考，不支持任何形式的决策依据，也不支撑任何形式的投资建议。本文是基于公众公司属性，根据其法定义务内向公众公开披露的财报、审计、公告等信息整理，不为未来的变化做背书，未来发生的任何变化均与本文无关。我们力求信息准确，但不保证其完整性、准确性、及时性。市场有风险，研究需谨慎。3）关于主题：财务建模报告工作量巨大，仅覆盖部分重点行业及案例，不保证您需要的所有案例都覆盖，请谅解。4）关于平台：优塾团队所有内容以微信平台为唯一出口，不为任何其他平台内容负责，对仿冒、侵权平台，我们保留法律追诉权力。