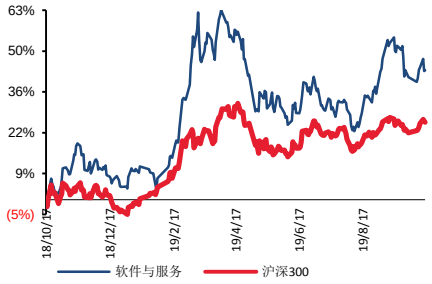
太平洋证券 PACIFIC SECURITIES

2019-10-17
行业深度报告
看好/维持
软件与服务

信息安全深度报告：政策、需求、格局变化下安全成长新周期

■ 走势比较



■ 子行业评级

相关研究报告：

《金山办公——基础软件自主创新榜样，移动端赛道领先》--2019/10/09

《华为生态正式进入投资时钟，行情震荡下紧抱核心主线资产》--2019/09/22

《交通建设纲要提出加强智能网联研发、形成自主可控完整产业链》--2019/09/19

证券分析师：王文龙

电话：021-61376587

E-MAIL：wangwenlong@tpyzq.com

执业资格证书编码：S1190517080001

报告摘要

市场自发性需求带动产品格局变化：服务和软件比例提升。

2016 至 2018 年间我国信息安全市场规模增速一直维持在 20%以上，2018 年市场规模达到 495 亿。国内安全市场硬件占比达到 61%，远高于美国 17%，全球 19%的硬件投资比例。随着云计算、工控、物联网的发展，信息安全行业需求激增，安全行业维度也随之扩展，预计软件及服务的占比将向全球平均水平靠拢。

周期+政策催化性需求促进局部领域行业快速增长。

19-20 年为十三五规划的最后两年，行业进入来自政府和军队采购的订单释放高峰期。十三五规划当中的关键分工，诸如构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，组织实施网络安全监测预警和应急处置工程均需由公安部牵头完成；军队部门的安全建设也是十三五规划当中重要的组成部分。

等保 2.0 将于 12 月 1 日正式推进，政策的推动高频且持续。相比于等保 1.0，在标准内容上，等保 2.0 从原本安全通用要求扩展到了通用要求+云计算、物联网、移动互联、工业控制和大数据等要求。在工作内容将互联网企业纳入等级保护管理，实现平台级的维护。全面提升极大的扩展了网络安全市场的上限，而由于安全要求细化，未来很难有公司一次性过保，大概率是分阶段，分层次的过单项审核，为网安公司开辟了广阔的市场空间和更长的成长周期。

龙头格局将在互相挤压中逐渐突破。

美国信息安全市场在经历长期竞争后，龙头赛门铁克市占率 15.2%，市场 CR5 达到 37.6%。而国内由于仅今年华为、华三、奇安信等厂商安全业务成长迅速，跻身一线行列，加剧竞争态势，同时国内单体公司的绝对量级和全球头部企业相差较大。目前，国有资本纷纷入局行业头部企业、互联网公司和硬件公司的介入都会对行业格局产生一定影响，而综合技术、销售、渠道、产品等多方面因素，头部集中、强者恒强是大概率的。相关公司：启明星辰、绿盟科技、深信服、紫光股份、美亚柏科、山石网科等。

风险提示

军队业务订单增长存在不确定性；安全运营中心业务竞争者增加，头部竞争格局激烈；等保 2.0 的实质性推进过程中对历史市占率的颠覆等。

目录

图表目录

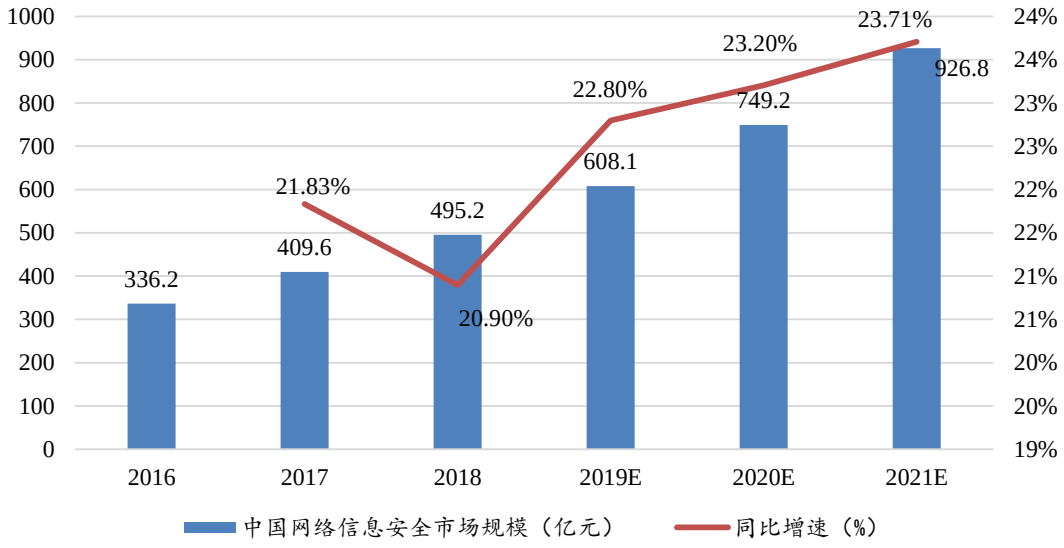
市场化自发性需求带动格局变化——软件、服务将成主流

目前我国信息安全市场安全投入占比较低、硬件投入比重较高。参照海外市场的信息安全投入占比以及我国十三五规划当中的IT投入计划，理想状态下未来三到五年中我国信息安全市场规模有三到四倍的增长空间。同时，参照海外安全市场投资结构，未来软件、服务将取代硬件成为行业发展的主要驱动力。

1）信息安全市场增速稳定,投资占比提升空间大

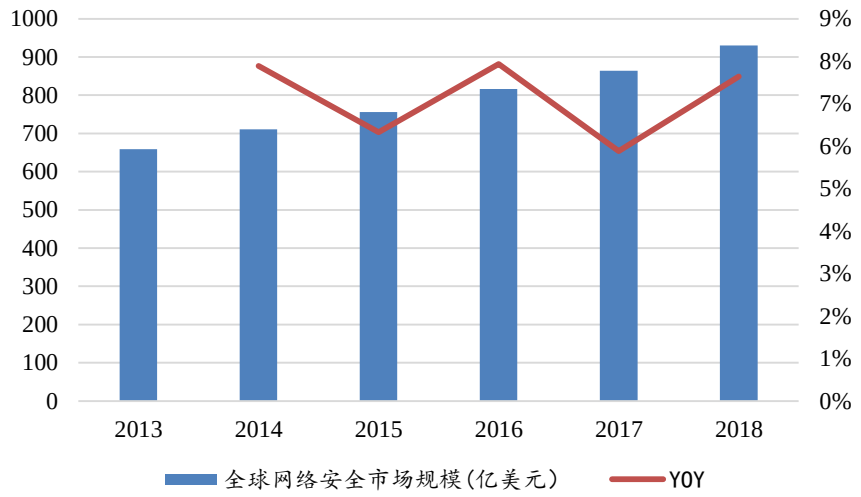
信息安全市场规模保持稳定增长。根据前瞻产业研究院的数据，2016至2018年间我国信息安全市场规模增速一直维持在20%以上的高速增长。2018年我国信息安全市场规模达到495亿，同比增长20.90%。对比全球网安市场7%的复合增速，我国网络安全市场仍然保持着较快的增长。

图表 1：2016-2021 年中国网安市场及预测



资料来源：前瞻产业研究院，太平洋证券整理

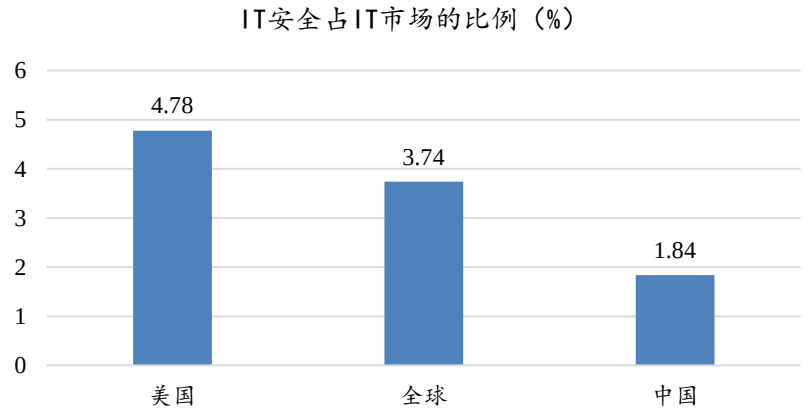
图表 2：全球信息安全市场增速趋于稳定



资料来源：智研咨询，太平洋证券整理

对标美国，我国信息安全市场增量广阔。我国现阶段信息安全市场建设量距离饱和尚远。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。根据《十三五”国家战略性新兴产业发展规划》，我国计划到2020年形成十万亿规模的信息技术行业，按照1.84%的市场占比推算，我国的信息安全市场尚有三到四倍的增长空间。未来随着安全投入偏好的提升，信息安全投入占比有望增加，市场空间将会得到投资占有率提升和IT总空间变大的双重扩展。

图表 3：中国网络安全投入占比偏低



资料来源：前瞻经济学人，IDC，太平洋证券整理

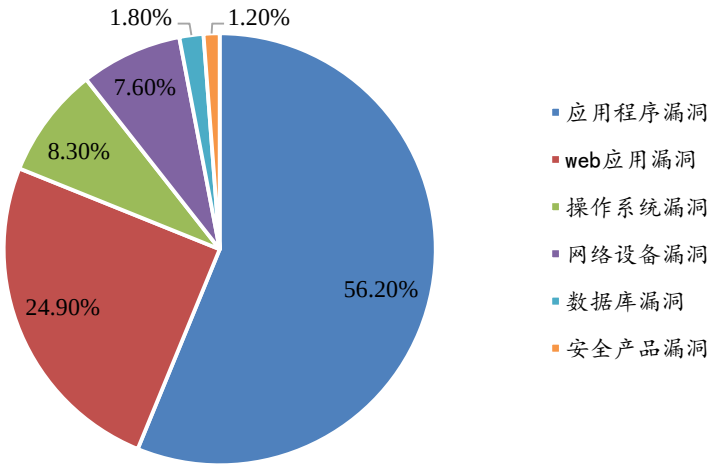
2）国内安全硬件占比偏高，软件、服务将成为行业增长驱动力

我国信息安全投入结构偏硬。根据IDC的数据，2018年我国信息安全投资当中，硬件投资占比61%，相比于美国17%和全球19%的占比明显偏高。软件和服务是信息安全领域的核心，中国市场安全投入偏硬，信息安全中的软件、服务投入被严重低估。

硬件占比偏高的原因在与安全投入理念的初级。在中国企业的传统观念当中，安全投入只需购买相关的安全服务硬件即可，对于后续服务的更新以及相关人才的培养仍然相对不重视。硬件占比偏高的情况预计将在我国网络安全市场长期存在。

应用程序漏洞占比大，安全漏洞涉及厂商众多。据CNVD统计，2019上半年收录的漏洞中，应用程序漏洞占比最大，高达56.2%，其次是Web应用漏洞和操作系统漏洞。安全漏洞主要涵盖Google、Microsoft、IBM、Oracle、Cisco、Foxit、Apple、Adobe等厂商产品，2018年与Google有关的安全漏洞数量最多，为693个，占全年收录数量近5%。

图表 4：2019 上半年 CNVD 收录漏洞按影响对象类型分类



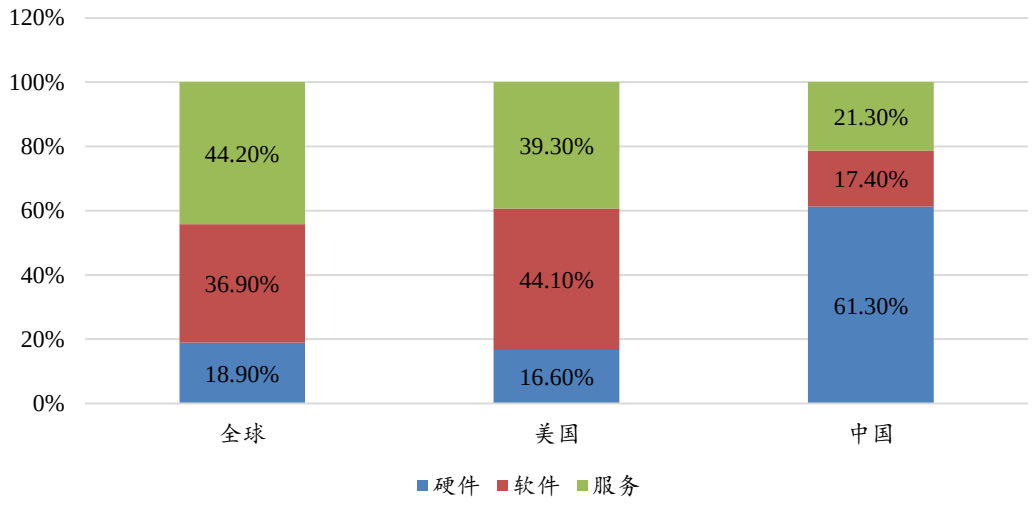
资料来源：CNVD，太平洋证券整理

图表 5：2018 年 CNVD 收录安全漏洞数量

漏洞涉及厂商	漏洞数量（个）	占全年收录数量百分比
Google	693	4.90%
Microsoft	667	4.70%
IBM	564	4.00%
Oracle	481	3.40%
Cisco	422	3.00%
Foxit	369	2.60%
Apple	367	2.60%
Adobe	352	2.50%
WordPress	261	1.80%
Linux	193	1.40%
其他	9832	69.20%

资料来源：CNCERT，太平洋证券整理

图表 6：中国网络安全投入，硬件占比偏高



资料来源：IDC，太平洋证券整理

3）云安全、工控安全等新增需求即将爆发

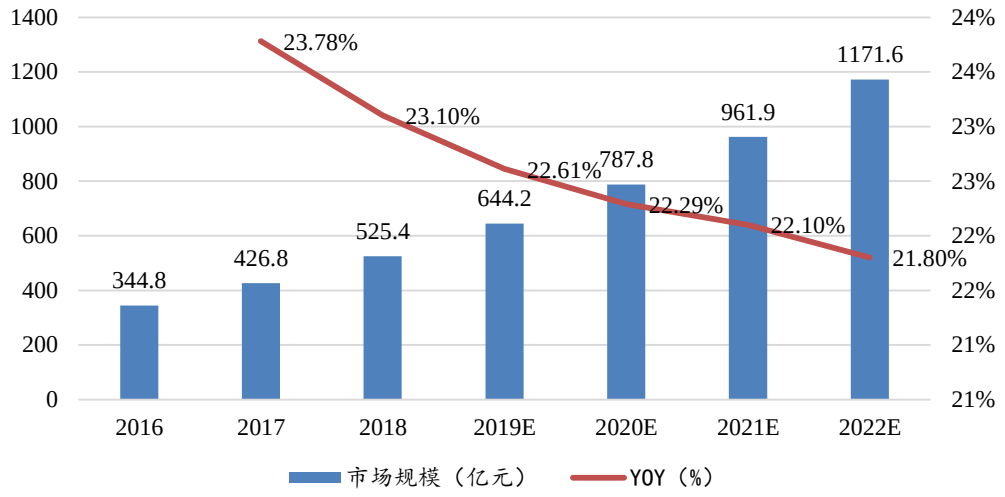
受等保2.0政策的影响以及云计算、物联网等新兴行业的发展，云、物联网等等新行业对于信息安全的需求得到拉升。由于新行业的特性，原先适用于传统安全领域的产品无法应用于新兴行业领域。新安全产品的推出将进一步扩展行业维度。分行业来看，云安全将从私有云领域率先爆发，而物联网的安全产品中工控安全、车联网安全将首先启动。

（1）云安全：市场规模迅速增长，私有云安全有望率先爆发

云计算高速增长，私有云占据云计算主体。由于云计算的成本优势，近年来我国云

计算市场规模高速增长。相比于公有云市场，我国私有云市场占云计算行业的主体。2017年我国私有云市场规模达到426亿元，同比增长23.48%。目前私有云渗透率在企业用户中仍然较低，未来私有云仍有较大的增长空间。

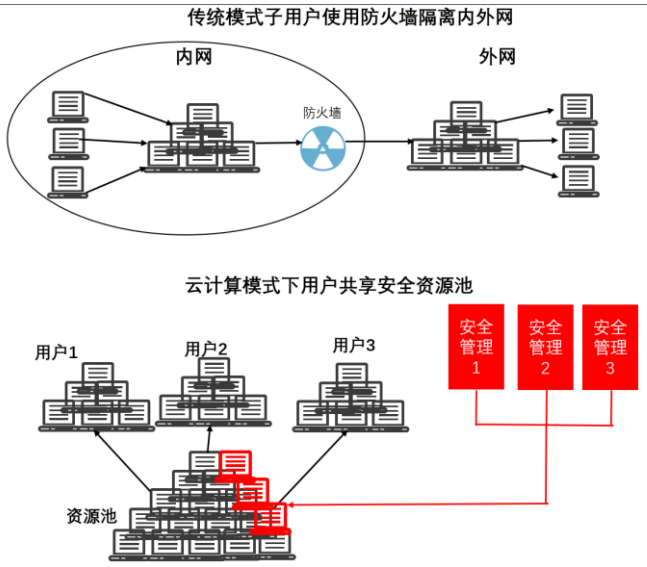
图表 7：中国私有云市场规模



资料来源：智研咨询，太平洋证券整理

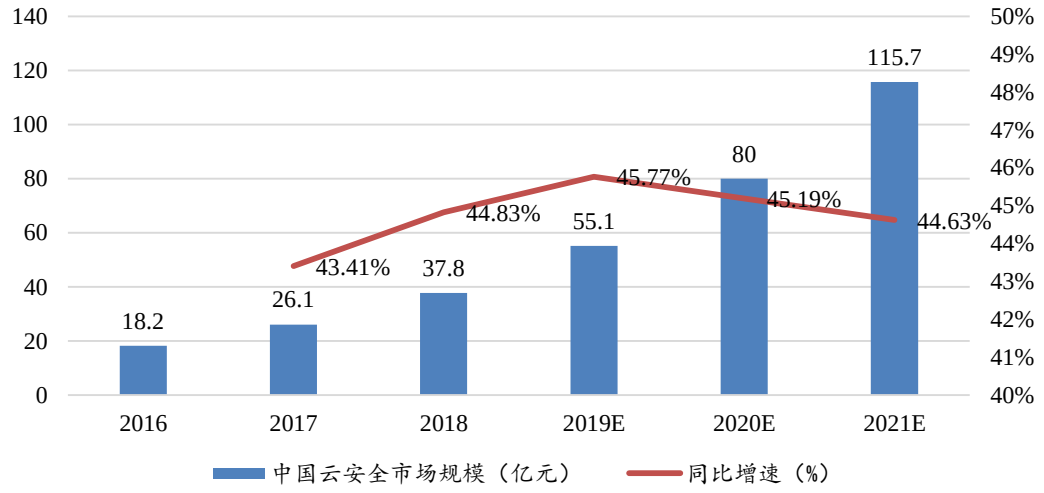
传统安全产品无法适用云计算，云安全需求得到拉升。由于云模式下用户共享安全资源池的特性，因此使用防火墙隔离危机的传统安全产品无法适用于云安全领域。针对云计算市场必须推出专用的云安全产品。等保2.0将云计算纳入等级保护对象，云计算的安全投入将成为合规性需求。云安全需求的扩张开辟了信息安全市场的新维度，云安全行业市场规模高速增长。我国云安全市场仍处于刚刚起步的高速增长阶段。根据智研咨询的数据，2016年我国云安全市场规模已经达到18.2亿美元，并保持了超过40%的增速的增长。云安全市场方兴未艾，未来随着私有云渗透率的进一步提高，云安全产品的市场份额将进一步提升。

图表 8：传统安全产品与云安全产品使用场景区别



资料来源：智研咨询，太平洋证券整理

图表 9：中国云安全市场规模高速增长



资料来源：前瞻产业研究院，太平洋证券整理

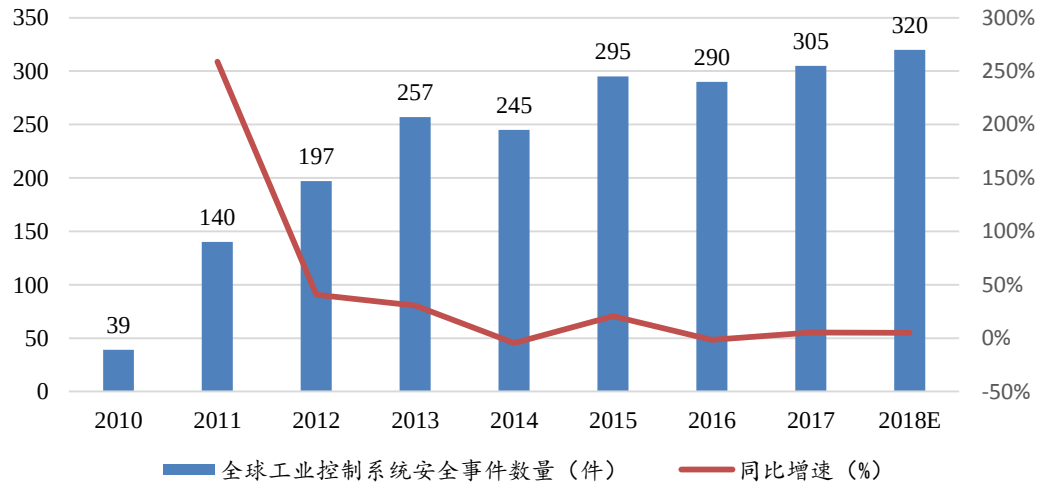
私有云安全市场有望首先爆发。目前我国私有云市场占云计算的市场份额的主体。由于公有云厂商大多自建安全系统，因此对于传统信息安全厂商的云安全产品的需求客户大多集中于私有云领域。政府、金融、军队等涉密等级较高的客户多数选择私有云，对于云安全的需求也更加旺盛。私有云硬件提供商（华为、华三等）不具备提供私有云安全服务的能力，而大型公有云厂商（阿里等）缺少与政府在私有云领域的合作经验，因此对于传统安全厂商来说，云安全业务有望首先在私有云领域实现爆发。预计未来云

计算市场的安全需求将率先从私有云安全爆发。

2）智能制造2.0推动物联网安全需求增长

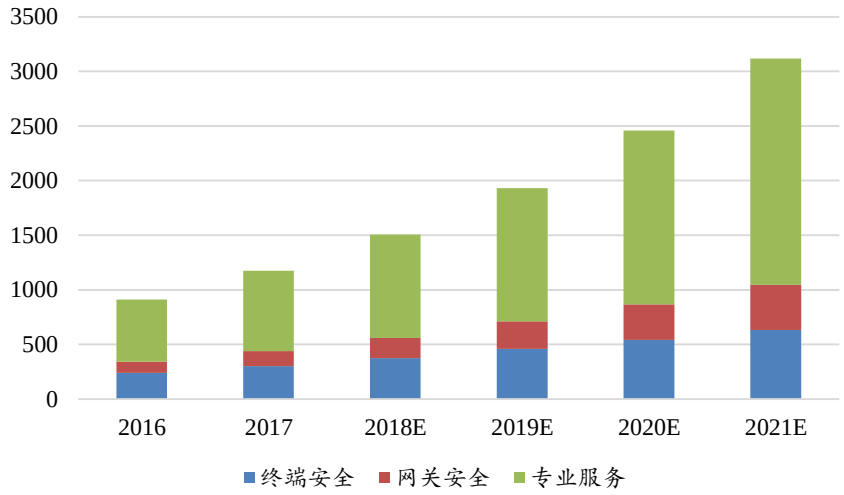
智能制造规模猛增，物联网安全迫在眉睫。2015年5月，我国发布《智能制造2025战略》，要求提升传统工业企业的智能化水平以及初步建立智能网联汽车的生产研发体系。2017年1月工信部发布《物联网“十三五”规划》，要求完善物联网技术创新体系，构建完善标准体系，推动物联网规模应用，完善公共服务体系，提升安全保障能力。物联网市场快速增长，而其安全形势却令人担忧。近年来，随着物联网市场的快速发展，物联网安全问题频发。根据ICS-CERT的数据显示，2016年我国工控系统网络应急小组响应的工控安全事故数达到290个，事故数量相比2010年的39个增长了6倍。全球物联网安全市场规模也在高速增长，Gartner预计2018年全球物联网安全支出将达到15亿美元，同比增长28%，预计2021年全球物联网安全支出将达到31.18亿美元。

图表 10：工控系统网络应急小组响应的工控安全事故数（个）



资料来源：ICS-CERT，太平洋证券整理

图表 11：全球物联网安全市场规模预测（百万美元）

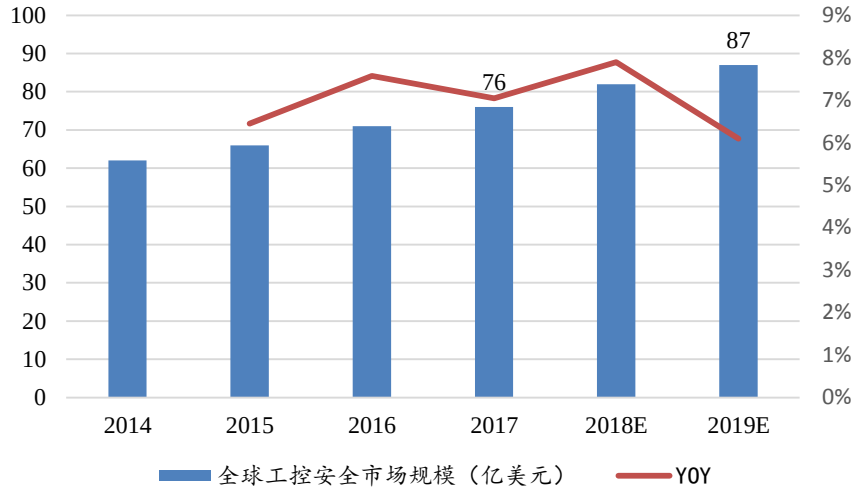


资料来源：Gartner，太平洋证券整理

物联网安全领域，工控、车联网安全有望率先落地。工控行业安全形势严峻，2018年上半年里41.2%的系统至少遭受过一次攻击，高于2017年上半年的36.6%（数据来源：电子发烧友）。以工控系统为代表的关键基础设施，是确保工业体系正常运转的神经中枢，也是工业领域各生产线稳定运行的根本。我国的工控系统主要应用于电力、能源、航空、轨道交通等行业，大多为关系到国计民生的关键行业，其对于安全投入的需求极为刚性。相关的工控安全政策已铺垫完善。2016年10月17日，工信部印发《工业控制系统信息安全防护指南》，明确了工控企业安全防护的指导方针；2016年10月13日，国家质量监督检验检疫总局、国家标准化管理委员会发布GB/T 33009工控安全标准，明确了工控安全的防护要求、管理要求、评估指南以及风险与脆弱性检测要求。2018年等保2.0的意见征求稿将工业领域纳入等级保护对象，工控领域的安全投入将成为合规性需求，工控安全将成为物联网安全率先落地的行业。从全球市场来看，工控安全市场规模增速稳定。2017年全球工控安全市场规模达到76亿美元，预计2019年市场规模将达到87亿美元。

车联网领域，根据相关机构的数据显示，目前普通汽车上有 25 到 200 个不等的 ECU（Electronic Control Unit，电子控制单元），而高级汽车则能高达 144 个 ECU，无人驾驶的软件代码超过 2 亿行，其复杂度远超传统汽车。车载系统复杂程度的提升，将极大程度的增加车辆被攻击的风险。由于车辆安全需求较为刚性，国外主要厂商诸如思科、NXP等公司在车联网安全领域均已开始布局。

图表 12：全球工控安全规模预测



资料来源：IDC，太平洋证券整理

周期+政策催化性需求——促进局部领域行业增长

信息安全投入属于纯成本，短期无法带来收益，广义上来说可以将信息安全行业的发展分为两类：一类为客户行业规模增长带来的信息安全固定投入增长（云计算发展、互联网行业发展等多行业规模提升带来的信息安全行业增长）。另一类为信息安全投入偏好增长所带来的信息安全市场增长（占总IT投入比例的增加）。固定投入的增长主要受客户所在行业发展驱动，而投入偏好的增长主要受如下驱动力驱动：采购周期驱动、政策驱动、安全事件驱动和需求驱动。

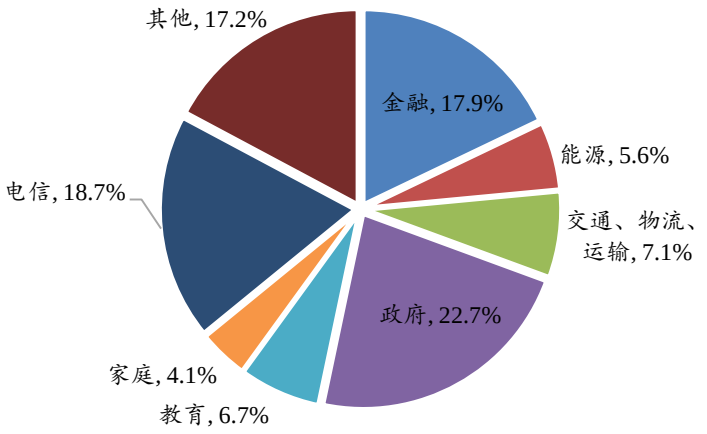
首先是采购周期驱动。根据历史数据，在五年规划的后两年中信息安全的采购比例会增加。目前我国处于五年计划的后两年当中，采购金额有望增加。其次分析后三类驱动。信息安全行业为纯成本投入无法带来收益，对于党政军以及国企用户而言，信息安全行业最直接的驱动力是安全政策落实从而增加信息安全的采购预算。安全事件驱动多为主题投资，**规模较小的安全事件对安全投入偏好的刺激不明显，只有大规模安全事件的爆发才会落实到安全行业的增长，比如今年的“护网行动”，即大规模安全事件促使需求和新的安全政策同步出现，从而驱动安全行业发展**。因此信息安全行业的驱动主要依靠政策驱动，政府采购周期的变化和对企业安全要求的标准影响信息安全行业增长的核心要素。

1）十三五规划末期，政府信息安全采购比例有望上升

信息安全行业客户多集中于政府部门，采购周期的变化对信息安全行业激励明显。网络安全行业的下游客户主要集中于电信、金融、政府三大行业，三大行业的采购份额占了信息安全市场份额的59.3%。其中，政府部门的采购占比最大，为22.7%，其余的金融、电信等部门大多为国有企业。信息安全投入为纯成本投入，行业规模的增长主要受采购预算增长的驱动。政府部门的采购主要依赖于国家政策规划的采购预算，而国有企业部门在信息安全行业的采购也很大程度上受国家政策的影响。通常在五年规划的末期政府对于信息安全相关的采购会达到高峰。

十三五计划要求构建关键信息基础设施安全保障体系。实施网络安全审查制度，防范重要信息技术产品和服务网络安全风险。关于细分行业，十三五计划要求加强金融、能源、水利、电力、通信、交通、地理信息等领域关键信息基础设施核心技术装备威胁感知和持续防御能力建设，增强网络安全防御能力和威慑能力。

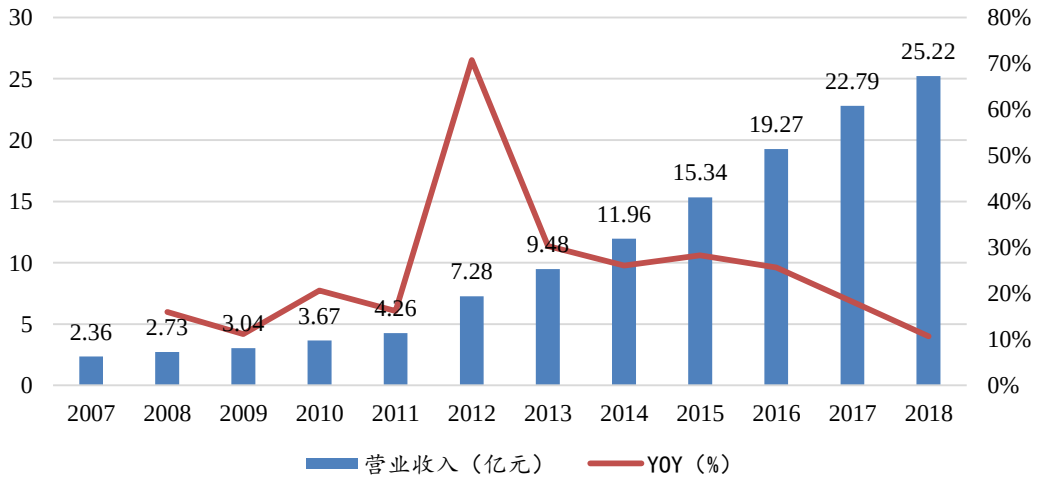
图表 13：2017 年信息安全行业下游客户分布



资料来源：智研咨询，太平洋证券整理

参照行业龙头启明星辰的收入情况，剔除其2012年并购网御星云后收入大幅增长的影响，其收入增速在2009-2010年，2014-2015年均有明显上升，其中09年和14年均为增速的拐点年份。

图表 14：五年规划末期公司收入增长明显（12 年为网御星云并表影响）



资料来源：公司财报，太平洋证券整理

军队、公安部门订单有望在未来两年恢复。十三五规划当中的关键分工，诸如构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，组织实施网络安全监测预警和应急处置工程均需由公安部牵头完成；军队部门的安全建设也是十三五规划

当中重要的组成部分。受十三五初期公安部门改革以及军队内部人员变化等原因的影响，军队、公安行业目前对于信息安全采购的订单较为低迷。以启明星辰为例，2018年军队相关的安全业务的收入有所下滑。十三五规划末期将至，军队与公安部门采购预算并未缩减。预计军队和公安部门的订单将在未来两年快速复苏。

2）等保 2.0 等政策出台持续刺激市场前进

信息安全形势依然严峻，刺激行业政策出台。2018年我国网络安全漏洞的数量总体有所下降，为14201个，同比减少12%。安全漏洞数量有所下降但仍处于高位，信息安全形势依然严峻。安全漏洞数量持续保持高位，网络安全防护涉及范围越来越广，由此带来的是安全事件的频发和大量的经济损失。根据Juniper research的研究分析预测，2019年网络犯罪造成的损失将高达2.1万亿美元，为2015年的四倍。2019年4月，哔哩哔哩后台工程源码遭整体泄露；2019年上半年，国家互联网应急中心发现我国境内40多家大型工业云平台持续遭受漏洞利用、暴力破解等网络攻击。基于云计算、物联网、移动互联、工业控制系统的网络安全问题是未来的核心，等保2.0对新型应用需求展开了针对性的覆盖。

图表 15：近期爆发的大规模安全事件

时间	事件
2019	今年 2-3 月份，Gnosticplayers 在暗网分四轮出售从 38 个热门网站窃取的 8.7 亿条用户信息。
	网络软件公司思杰 6-10TB 敏感数据遭窃取。
	IT 安全和云数据巨头 Rubrik 数据库泄露。
2018	美国约 300 所大学遭受黑客攻击，黑客窃取了 31TB 的数据，以及预估价值 30 亿美元的知识产权信息。
	Intel 处理器被曝光存在漏洞。
	Under Armour 的健康和健身追踪应用 MyFitnessPal 遭到黑客攻击，大约有 1.5 亿用户受到影响，泄露的信息包括用户名、电子邮件地址以及密码等。
2017	俄罗斯电网遭到 NotPetya 勒索软件攻击。
	法国总统马克龙的竞选团队宣布，他们遭到“大规模”电脑黑客袭击，竞选邮件被黑客盗窃，上传到了网上。
	加拿大贝尔公司，约 190 万个活跃电邮地址、1700 个客户姓名以及在用电话号码遭到匿名黑客的非法入侵。
2016	黑客攻击 SWIFT 系统盗窃孟加拉国央行 8100 万美元。
	俄罗斯央行遭黑客攻击 3100 万美元不翼而飞。
	美国遭史上最大规模 DDoS 攻击、东海岸网站集体瘫痪。
	雅虎宣称其至少 5 亿条用户信息被黑客盗取。
2015	大麦网 600 多万用户账号密码泄露数据被售卖。
	加拿大婚外情网站 Ashley Madison 遭遇黑客攻击，导致数百万用户的信息泄露。
	美国第二大医疗保险公司 Anthem，被黑客入侵并盗走 8000 万个人信息。
2014	全球最大的比特币交易平台 Mt.Gox 75 万个比特币被窃，损失估计达到 4.67 亿美元，被迫宣布破产。
	2014 年 4 月，国内某黑客对国内两个大型物流公司的内部系统发起网络攻击，非法获取快递用户个人信息 1400 多万条。
2013	斯诺登曝光棱镜计划。

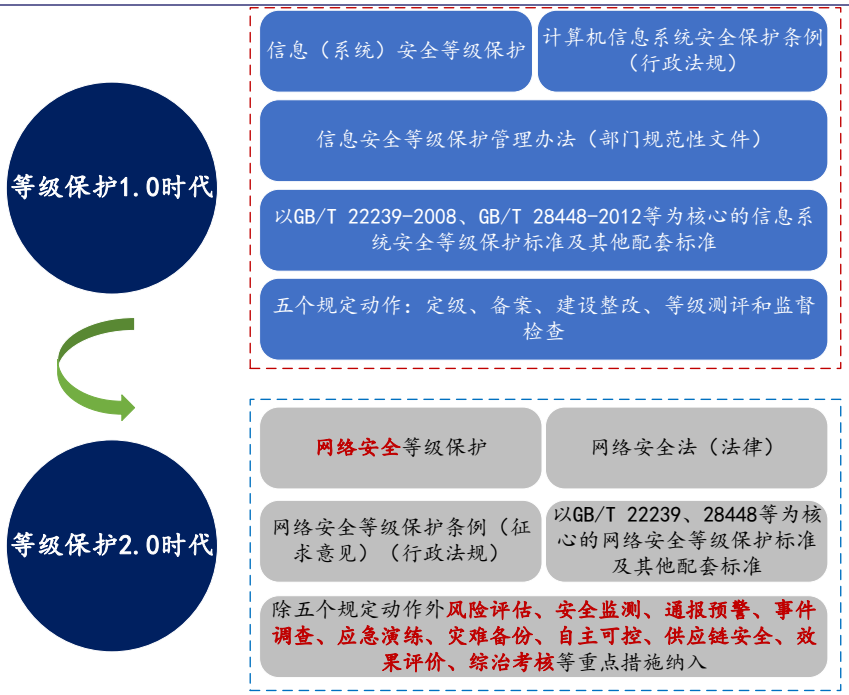
资料来源：公开资料整理，太平洋证券整理

网安法确立法律基础，等保2.0扩展行业维度。2017年6月1日网安法正式开始实施，从网络运营安全、网络信息安全以及关键信息基础设施建设保护三个方面明确了网络安全保护的具体措施。网安法首次从法律层面明确了网络安全的重要性，为网安市场的发展铺垫了稳定的政策环境。2018年公安部《网络安全等级保护条例（征求意见稿）》，对网络进行五个安全等级的划分，适用范围相比于等级保护1.0有了明显的扩大。此外，在细分行业中网络安全相关的辅助配套细则也在2018年逐渐出台。等保2.0将于12月1日正式推进落地也将极大促进网络安全市场的发展。

等保2.0提升行业维度，拓展行业上限空间。相比于等保1.0，在标准内容上，等保2.0从原本安全通用要求扩展到了通用要求+云计算、物联网、移动互联、工业控制和大

数据等要求。在服务对象维度，等保2.0从原本的计算机信息系统+网络安全基础设施维度扩展到了+云、移动互联网、物联网、工业控制系统、大数据安全等对象维度。在工作内容将互联网企业纳入等级保护管理，实现平台级的维护。全面提升极大的扩展了网络安全市场的上限，而由于安全要求细化，未来很难有公司一次性过保，大概率是分阶段，分层次的过单项审核，为网安公司开辟了广阔的市场空间和更长的成长周期。

图表 16：从等保 1.0 到等保 2.0



资料来源：公开资料整理，太平洋证券整理

图表 17：等保 1.0 和 2.0 的《基本要求》差异

《基本要求》1.0（三级通用要求）	安全控制点	安全要求项
物理安全	10	32
网络安全	7	33
主机安全	8	32
应用安全	8	31
数据安全	3	8
安全管理制度	3	11
安全管理机构	5	20
人员安全管理	5	16
系统建设管理	11	45
系统运维管理	13	62

《基本要求》2.0（三级通用要求）	安全控制点	安全要求项
安全物理环境	10	22
安全通信网络	3	8
安全区域边界	6	20
安全计算环境	11	34
安全管理中心	4	12
安全管理制度	4	7
安全管理机构	5	14
安全人员管理	4	12
安全建设管理	10	34
安全运维管理	14	48

资料来源：公开资料整理，太平洋证券整理

图表 18:《基本要求》扩展部分

云计算安全扩展要求	移动互联安全扩展要求	物联网安全扩展要求	工业控制系统安全扩展要求
主要增加内容包括“基础设施的位置”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。	主要增加的内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等方面。	主要增加的内容包括“感知节点的物理防护”、“感知节点的设备安全”、“感知网关节点设备安全”、“感知节点地管理”和“数据融合处理”等方面。	主要增加的内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等方面，针对工业控制系统实时性要求高的特点调整了“漏洞和风险管理”和“恶意代码防范管理“等方面的要求。

资料来源：公开资料整理，太平洋证券整理

图表 19：网络信息安全政策梳理

时间	部门	文件	内容
2012	国务院	《关于大力推进信息化发展和切实保障信息安全的若干意见》	大力推进信息发展，切实保障信息安全。
2014	中央军委	《关于进一步加强军队信息安全工作的意见》	把信息安全工作作为军事斗争准备的保底工程，强力推进国产自主化建设应用，夯实信息安全根基。
2015.07	全国人大	《中华人民共和国国家安全法》	以法律形式确立了国家安全领导体质和总体国家安全观的指导地位。
2016.11	全国人大	《中华人民共和国网络安全法》	于 2017 年 6 月 1 日实施，从网络运营安全、网络信息安全以及关键信息基础设施建设保护等三个方面，就相关责任方、管理措施和技术措施等三个维度总结了具体实施要点。
2016.12	中央网络安全和信息化领导小组	《国家网络空间安全战略》	强调维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措。
2017.01	工信部	《软件和信息技术服务业发展规划》	首次明确提出信息安全产品收入目标,即到十三五末达到 2000 亿元，年增长率达到 20%以上。
2017.06	网信办	《国家安全事件应急预案》	预案将网络安全事件分为四级，明确网络安全事件应急处置工作实行工作机制。
2017.12	工信部	《工业控制系统信息安全行动计划(2018-2020)》	目标到 2020 年，全系统工控安全管理工作体系基本建立，全社会工控安全意识明显增强。建成全国在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（一网一库三平台），态势感知、安全防护、应急处路能力显著提升。培育一批影响力大、竞争力强的龙头骨干企业，创建 3-5 个国家新型工业化产业示范基地（工业信息安全），产业创新发展能力大幅提高。

资料来源：公开资料整理，太平洋证券整理

图表 20：网络信息安全政策梳理（续）

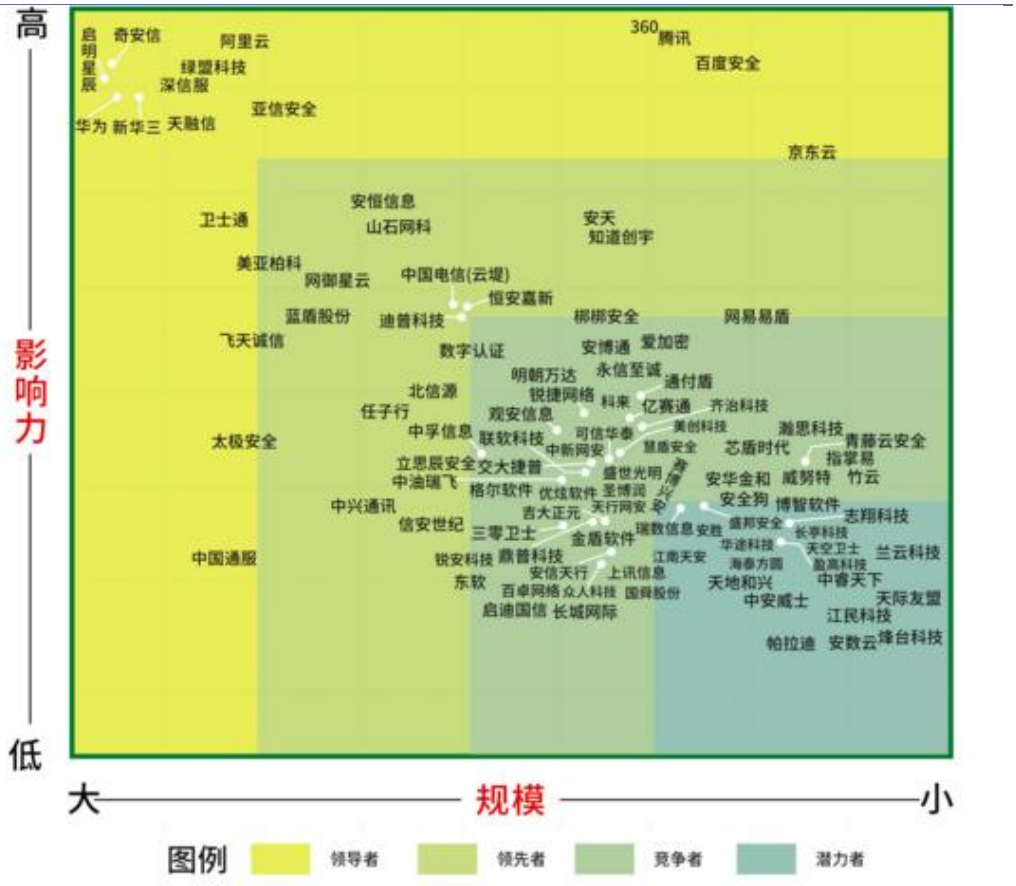
时间	部门	文件	内容
2018.03	农业部	《2018 年农业部网络安全与信息化工作要点》	首次将网络安全和信息化并列。提出建立健全农业部网络安全管理制度体系和工作机制。把网络安全纳入绩效考核指标。提出要提升网络安全防护能力、提升网络安全态势感知能力、提升网络安全应急处路能力。
2018.03	教育部办公厅	《2018 年教育信息化和网络安全工作要点》	首次将网络安全和信息化并列。提出进一步提升网络安全人才培养能力和防护水平、提高教育系统网络安全保障能力
2018.04	上海市经信委	《上海市工业控制系统信息安全行动计划（2018—2020 年）》	目标到 2020 年形成服务联络千家企业、督促指导百家重点企业的工作网络，在全市树立 10 家工控安全体系化标杆企业，打造 40 家安全评估示范工厂。同时重点培育 3-5 家本地技术支撑机构，建成工控系统安全综合管理系统。创建国家级工业信息安全主题产业园，引进和培育一批影响力大、竞争力强的龙头骨干企业，实施一批技术创新和成果转化项目，打造工控系统信息安全技术产业高地。
2018.06	公安部	《网络安全等级保护条例（征求意见稿）》	对网络进行五个安全等级的划分，对不同安全等级的网络提出了不同要求。相对于之前的等保 1.0，等保 2.0 适用范围扩大，所有网络运营者都要进行对相关网络开展等保工作。
2018.11	公安部网络安全保卫局	《互联网个人信息安全保护指引（征求意见稿）》	从管理机制、技术措施和业务流程三个方面指导互联网企业建立健全个人信息安全保护的安全管理机制和技术措施。
2019.05	全国信息安全标准化技术委员会	《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》	等级保护的基本要求、测评要求和安全设计技术要求框架统一，即：安全管理中心支持下的三重防护结构框架。 通用安全要求+新型应用安全扩展要求，将云计算、移动互联、物联网、工业控制系统等列入标准规范。 将可信验证列入各级别和各环节的主要功能要求。
2019.05	国家互联网信息办公室	《数据安全管理办法(征求意见稿)》	征求意见稿以个人信息和重要数据为主要管理对象，创新性地提出了备案制要求，并针对默认授权、功能捆绑、爬虫等互联网企业的常见做法做出了约束。
2019.06	工信部	《国家网络安全产业发展规划》	到 2025 年，依托产业园建成我国网络安全产业“五个基地”：一是国家安全战略支撑基地。二是国际领先的网络安全研发基地。三是网络安全高端产业集聚示范基地。四是网络安全领军人才培育基地。五是网络安全产业制度创新基地。
2019.09	工信部	《关于促进网络安全产业发展 的指导意见(征求意见稿）》	提出了五大主要任务，分别是：着力突破网络安全关键技术、积极创新网络安全服务模式、合力打造网络安全产业生态、大力推广网络安全技术应用以及加快构建网络安全基础设施。

资料来源：公开资料整理，太平洋证券整理

龙头格局将在相互挤压中逐渐突破

由于信息安全市场细分行业多、单个细分领域市场规模较低的原因，我国信息安全市场的格局目前较为分散。目前行业内龙头公司大多以选择上市巩固其行业地位，未来随着云安全、物联网安全的兴起，行业竞争格局将发生变化，行业内的龙头厂商将进一步发挥自身的渠道以及技术优势提升市场份额，行业集中度将逐步提升。此外，行业客户市场以华为、华三、360等为代表的新进入的竞争者威胁明显，传统网安行业的龙头公司份额或受到挤压和挑战。

图表 21：2019 年中国网安市场百强企业



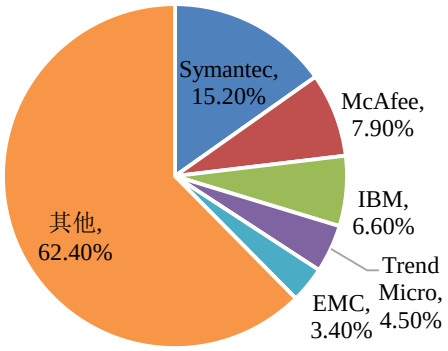
资料来源：安全牛，太平洋证券整理

1）中国网安市场集中度仍有较大提升空间

对比海外市场，我国信息安全市场极为分散，龙头增长空间广阔。根据IDC的数据，

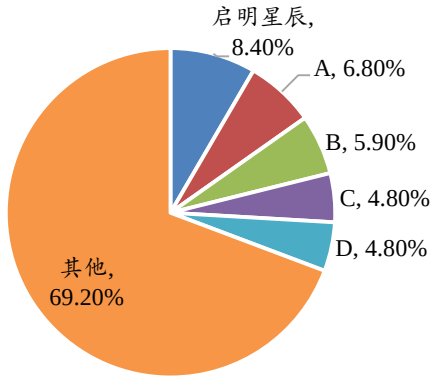
2015年启明星辰（包括子公司网御星云）为我国信息安全市场龙头，市场份额为8.4%，CR5为30.8%。对比美国信息安全市场，赛门铁克为市场龙头，市场份额15.2%，市场CR5为37.6%。虽然CR5份额相差不大，但是龙头公司的市场份额相差近一倍。对标美国市场，中国信息安全市场龙头份额仍然偏低。但是，新进入竞争者在威胁着传统网安龙头公司的市场份额，传统网安公司的市场份额受到威胁。

图表 22：2015 年全球网络安全市场格局



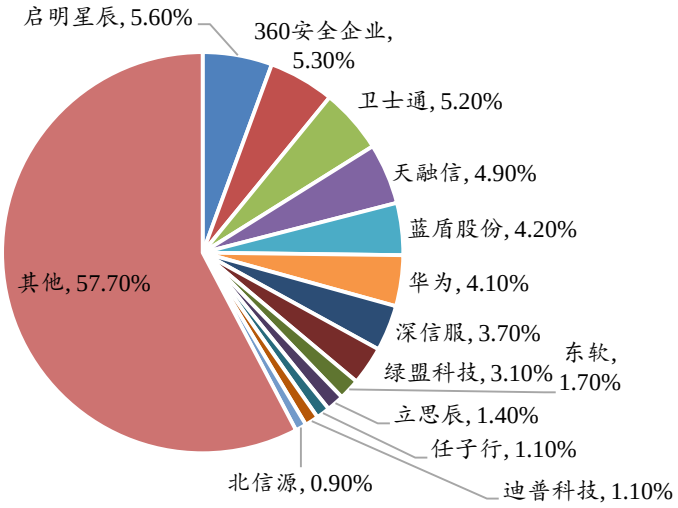
资料来源：IDC、太平洋证券整理

图表 23：2015 年中国网络安全市场格局



资料来源：IDC，太平洋证券整理

图表 24：2017 年中国网络信息安全产品品牌市场结构



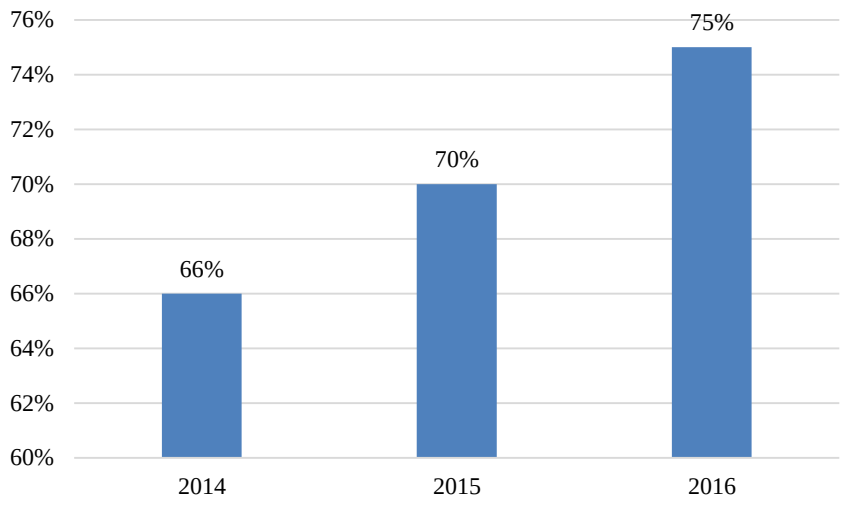
资料来源：赛迪顾问，太平洋证券整理

2）传统安全领域：行业集中度提升，头部厂商竞争激烈

传统安全产品的市场集中度进一步提升。安全行业下游客户的采购相对稳定，采购延续性好，在选定一家安全公司的产品后一般不会进行后续更换。由于信息安全行业的下游客户主体为政府、金融、电信行业，其采购来源相对固定，在安全行业长期耕耘的龙头公司有较大的渠道优势。此外，行业龙头企业拥有较强的技术以及资金优势，资源向行业龙头进一步集中。以防火墙市场为例，防火墙市场的CR5从2014年的66%提升至2016年的75%，行业集中度快速提升，资源进一步向头部厂商集中。

行业竞争白热化。由于传统安全市场以硬件销售为主，产品差别较小，主要依靠低价销售策略。小公司逐渐丧失竞争优势，行业向龙头集中。同时，由于传统安全领域解决方案趋同化严重，行业龙头之间的竞争也愈发激烈。以防火墙市场为例，根据IDC的数据，防火墙龙头天融信的市场份额从2015年的22.5%下降到2016年的21%。传统安全市场的竞争愈发白热化。

图表 25：中国防火墙市场 CR5 逐步提升

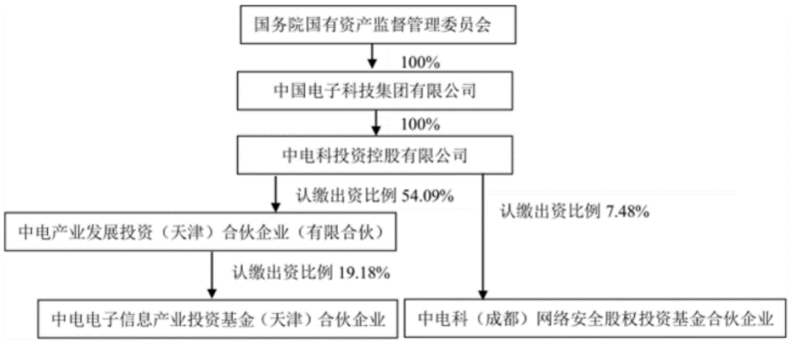


资料来源：IDC，太平洋证券整理

3）行业格局参与者开始国有化趋势，加速在安可、党政军领域的统治力

中国电科成为绿盟科技实际第一大股东。2019年2月，中国电科发起成立的产业基金中电基金和网安基金取得公司股权13.89%；2019年7月，中国电科全资子公司电科投资又增持绿盟科技股份。至此，电科投资及中电基金、网安基金合计持有公司股份1.24亿股，占公司总股本的15.50%，为公司第一大股东。

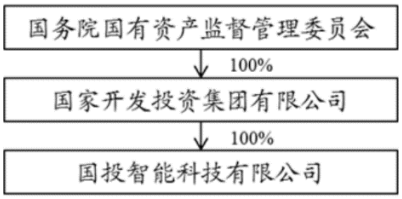
图表 26：中电基金、网安基金情况



资料来源:公司公告，太平洋证券整理

国投智能成为美亚柏科控股股东。2019年3月，国投智能出资19.44亿元，以每股15.49元的受让价格取得美亚柏科15.60%的股权和22.32%股份表决权，成为公司控股股东，国务院国资委成为公司的实际控制人。

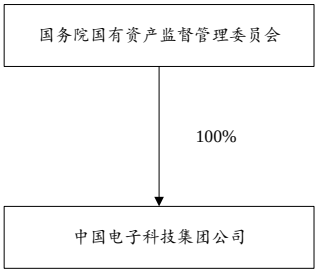
图表 27：国投智能股权结构



资料来源:公司公告，太平洋证券整理

中国电子战略入股奇安信。2019年5月，中国电子与奇安信签署战略合作协议，以37.31亿元持奇安信22.59%股份，成为其第二大股东，有望实现本质安全与过程安全深度融合。

图表 28：中国电子股权结构



资料来源:公司公告，太平洋证券整理

蓝盾股份获国资战略入股。2019年10月，科学城集团拟受让公司实际控制人柯宗庆先生、柯宗贵先生及其一致行动人中经汇通持有的蓝盾股份合计1.74亿股股票，总转股数占公司目前总股本将超过13%。转让完成后，科学城集团将成为公司第二大股东。

附注：科学城集团是广州经济技术开发区管理委员会出资成立的国有独资公司。

四川国资旗下全资子公司川投信产入股东方网力。2019年3月，川投信产受让公司股份6,388.52万股，持股比例为7.48%，成为公司控股股东。

4）对标美国，中国 2B 物联网公司增长空间有限

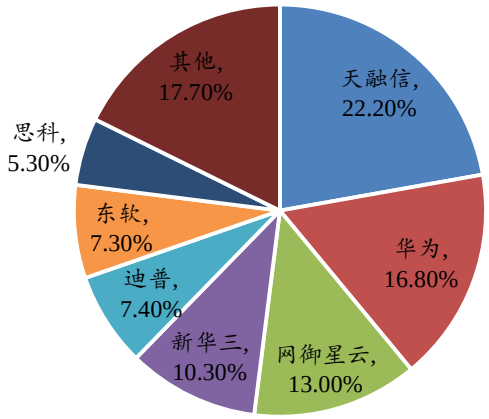
目前网络安全厂商的阵营横向纵向大致可以分为四类。第一类，是只做2B业务的软件为主的网络安全厂商，中国的代表厂商为绿盟科技、启明星辰。第二类是从硬件业务切入到网络安全市场的2B厂商，其业务主要以网络安全硬件为主，中国的代表为华为、华三等，美国代表厂商主要包括思科等。第三类为2B\2C业务均有涉足的网络安全软件厂商，中国代表厂商主要包括360等，海外代表厂商主要包括赛门铁克、checkpoint等。第四类是2B\2C业务均有涉足的网络安全硬件厂商，美国的代表主要为IBM等。

纯2B网安软件厂商稳步增长为主。对标中美网安厂商，中国A股目前的网络安全厂商除了360之外，其余厂商均为2B业务为主，业务也较少涉及硬件销售，主要以软件服务以及整体解决方案为主。而美股网络安全软件厂商主要包括赛门铁克、checkpoint等，其业务均涉及2C。造成中美网络安全软件公司业务方向的差异主要由于两方面，第一是个人安全软件付费习惯的差异。由于360的个人免费网络安全软件在国内的普及，国内个人用户对于网络安全软件仍未形成付费习惯，而美国的个人网络安全软件，包括赛门铁克等软件均需要付费服务。**第二，在美股市场，纯2B的网络安全公司市场竞争较为激烈，其需要向2C市场进行拓展以保证业务增长。**由于缺乏美股2B网络安全市场的相关数据，此处以中国2B网络安全市场为例。从防火墙市场和UTM市场来看，市场龙头的份额受后续竞争中挤压较为严重，市场竞争较为激烈。防火墙市场龙头天融信的市场份额从2015年的22.2%下降到2016年的20.9%，到18年恢复至22.4%，而网络安全硬件厂商华为、华三等市场份额落后的竞争中则奋起直追，华为从15年16%上升至18年21%，华三从15年10%上升为18年19%，而其他厂商的占比相对下降，市场头部区域明显挤压到靠后厂商的份额。通用软件厂商的网域星云的市场份额虽有提升，但是提升幅度相较网络安全硬件厂商较小。UTM市场龙头网域星云的市场份额也略有下降。新进入竞争者深信服、360企业安全等软件厂商则奋起直追。可见，纯2B的头部网络安全厂商市场份额受其竞争者挤压较为严重。由于中国网络安全市场的增速相对稳健，我们判断，未来国内信息安全

格局

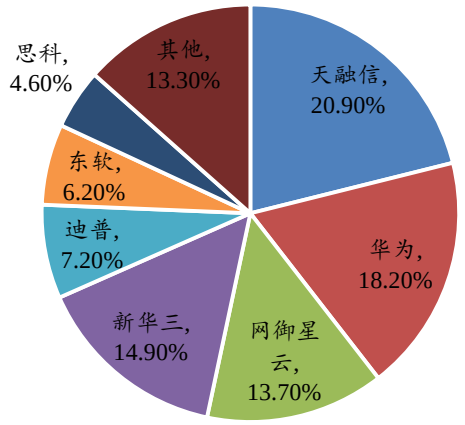
上将呈现，**传统安全厂商仅头部企业保住份额，二线开始掉队，华为、华三、奇安信等硬件厂商和互联网背景厂商会长期栖身第一梯队。**

图表 29：2015 年中国防火墙市场份额



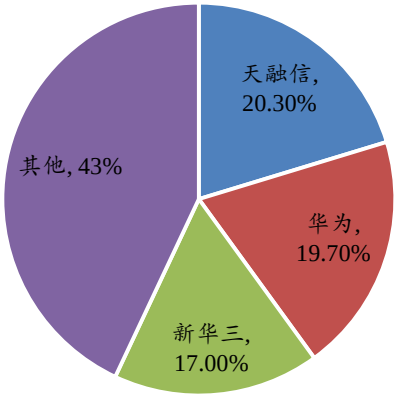
资料来源：IDC、太平洋证券整理

图表 30：2016 年中国防火墙市场份额



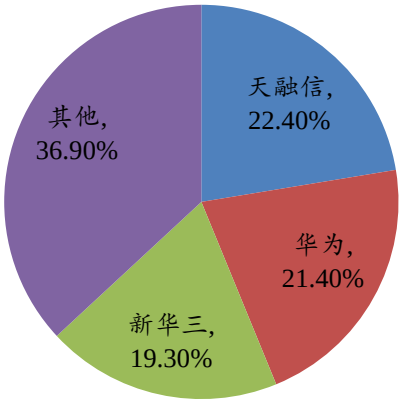
资料来源：IDC，太平洋证券整理

图表 31：2017 年中国防火墙市场份额



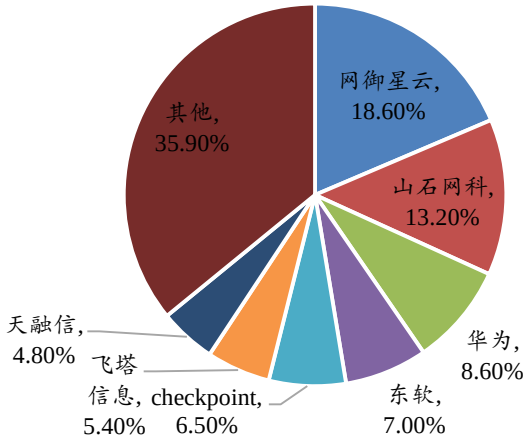
资料来源：IDC、太平洋证券整理

图表 32：2018 年中国防火墙市场份额



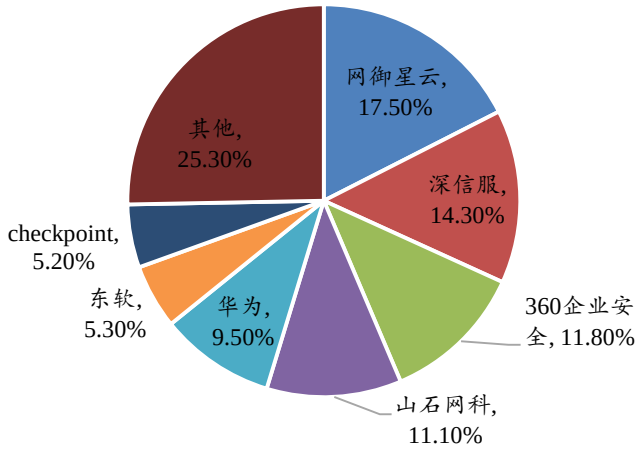
资料来源：IDC，太平洋证券整理

图表 33：2015 年 UTM 市场份额



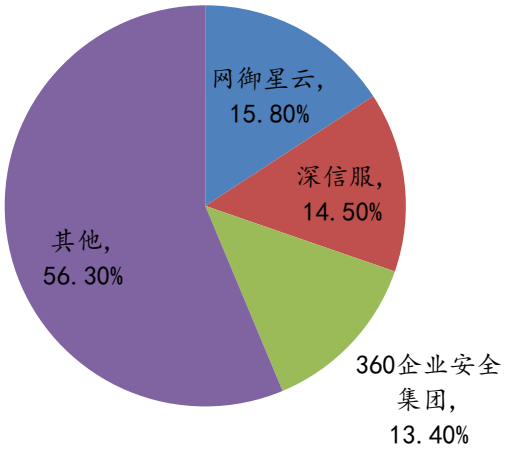
资料来源：IDC、太平洋证券整理

图表 34：2016 年 UTM 市场份额



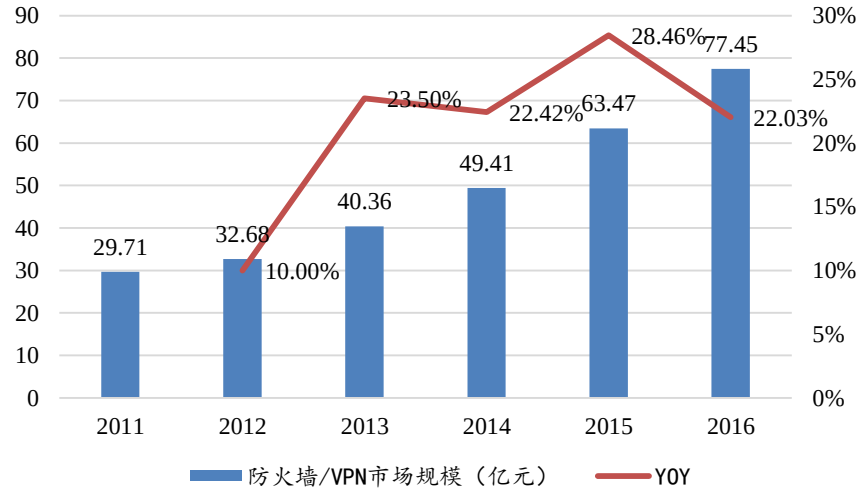
资料来源：IDC，太平洋证券整理

图表 35：2017 年 UTM 市场份额



资料来源：IDC，太平洋证券整理

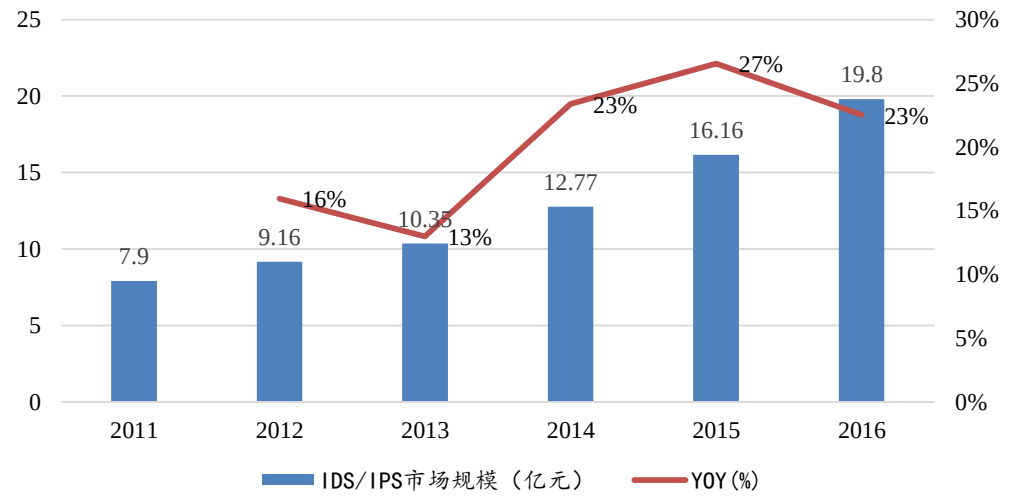
图表 36：防火墙市场规模增速趋于稳定



资料来源：智研咨询，太平洋证券整理

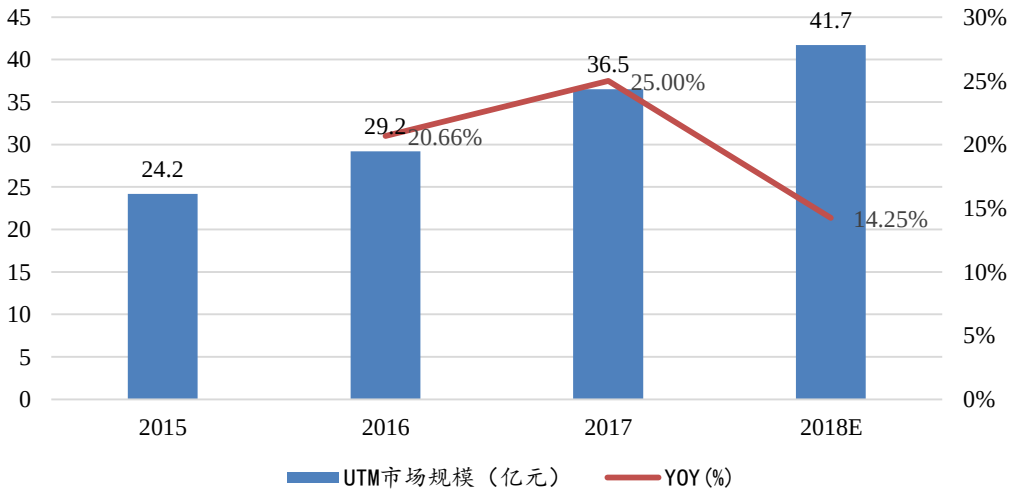
拓展新兴市场或为目前A股网安厂商转型方向。由于传统网络安全市场的增速日趋放缓，新进入者的竞争也愈发激烈，传统2B的网络安全软件厂商收入增速不同程度的出现了放缓。传统2B网安软件厂商通常由三类转型方向，一为拓展2C业务，二为进军硬件领域，三为布局新兴市场。关于转型2C业务，由于中美个人用户付费习惯的差异，短期内A股网安公司拓展2C业务存在着较大的困难。关于转型硬件厂商，由于硬件厂商的市场竞争更加激烈，市场格局已经区域稳定，传统网安厂商转型硬件几乎无可能。为了保证其在网络安全领域的竞争力，向新兴网安市场布局或为A股网安的公司的转型方向。以IDS/IPS市场和SOC市场为例，其市场增速虽已经逐步放缓，但市场格局仍然较为分散。2016年IDS市场的CR5为57%，相比于UTM市场的64%较低，龙头仍有扩展业务的空间。此外，云安全、工控安全的新型安全领域市场空间极为广阔，传统厂商的新兴业务转型仍然存在较大的空间。

图表 37：IDS/IPS 市场规模保持稳定增长



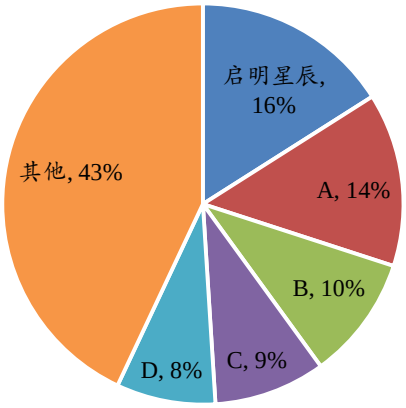
资料来源：智妍咨询，太平洋证券整理

图表 38：UTM 市场规模增速有所放缓



资料来源：中研普华产业研究院，太平洋证券整理

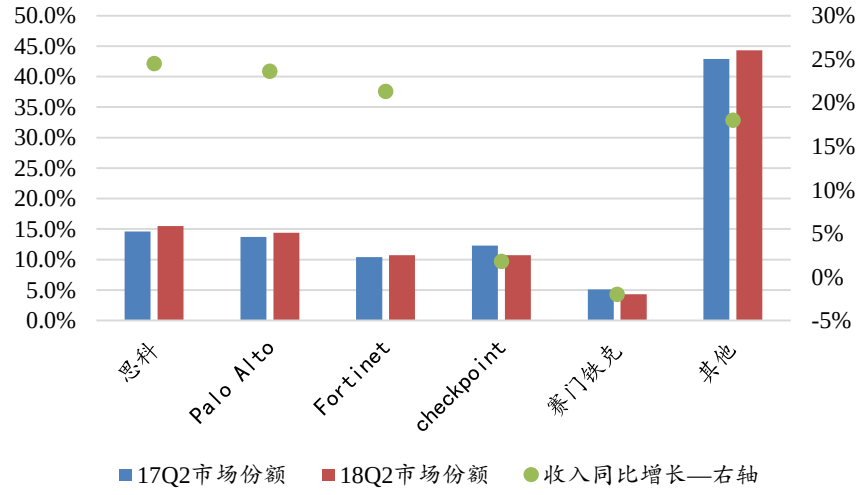
图表 39： IDS/IPS 市场集中度较低



资料来源：启明星辰官网，太平洋证券整理

以硬件切入网络安全领域的厂商优势较为明显。以美国市场为例，硬件驱动的网安公司市场份额处于龙头地位，且马太效应较为明显。思科为美国安全一体机市场龙头，其市场份额保持增长态势。而checkpoint、赛门铁克等软件为主的公司，市场份额均出现了不同程度的下滑。就中国市场而言，在传统安全领域，华为、华三的硬件驱动的网络安全公司，市场份额均保持着较为迅猛的增长。原因在于**硬件厂商相比软件厂商先天存在优势。**可以将硬件理解为IaaS层，软件和解决方案处于PaaS和SaaS层。硬件厂商先天占据了基础硬件层的优势，能够依靠基础层的优势更为有效的扩展市场份额。此外，硬件领域的厂商竞争相较软件领域更为激烈，硬件市场经历了数年的发展已经区域成熟，头部厂商地位较为稳定，软件厂商较难涉足硬件领域。硬件驱动的网安公司相较于软件驱动公司更具有竞争力。此外，目前中国的网络安全市场消费仍以硬件为主，硬件销售驱动型的网络安全厂商相较于软件驱动厂商存在较大的增长空间。

图表 40：美国安全一体机市场情况



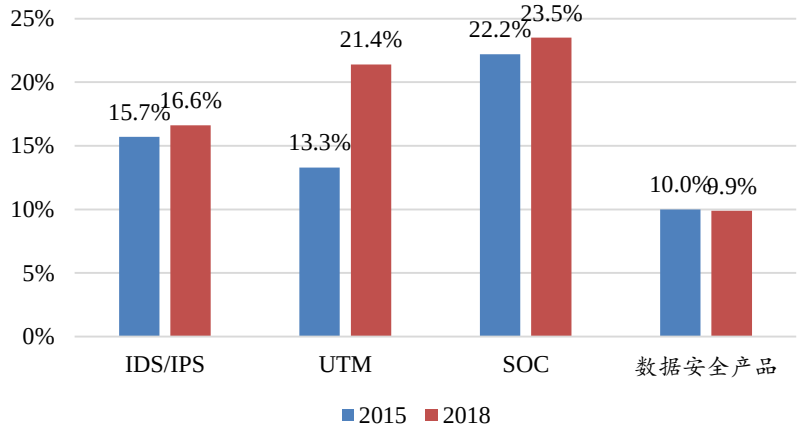
资料来源：IDC，太平洋证券整理

重点公司

启明星辰：传统网安龙头，安全运营中心模式锦上添花

公司产品线齐全，多项细分领域市占率常年保持第一。公司信息安全产品线齐备，包含传统网安产品如安全防护、监测、应用安全和数据安全，以及云安全、工控安全产品。赛迪顾问《2018-2019年中国网络信息安全市场研究年度报告》显示，启明星辰以5.1%的市场份额排在市场第一位，并且在传统网安的多个细分领域产品保持常年领先的状态：IDS/IPS产品连续17年排在市场第一，UTM产品连续12年排在市场第一位，安全管理平台SOC连续11年市场第一，数据安全产品连续4年市场排名第一。在工业互联网安全领域，公司与网御星云双品牌工业防火墙(IFW)在国内占有29.8%的市场份额，公司充分发挥know-how能力实现领跑。

图表 41：启明星辰多个细分领域常年保持第一



资料来源：CCID，太平洋证券整理

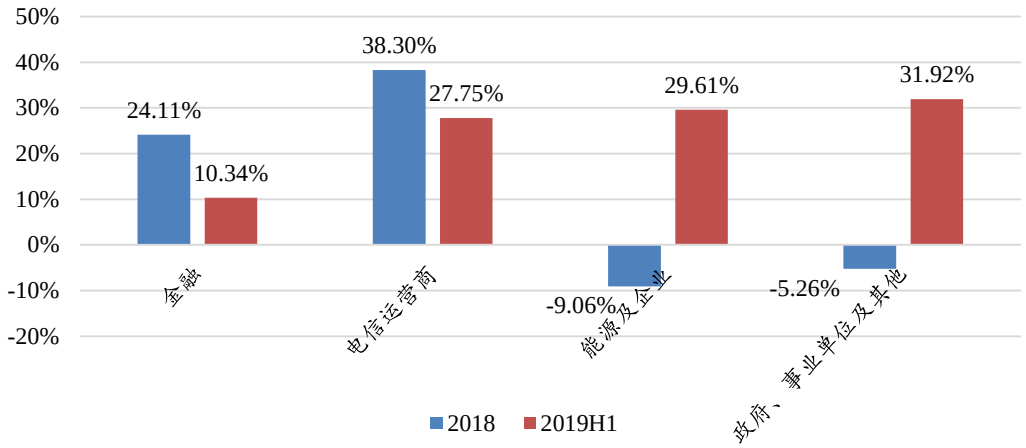
公司提出安全运营中心战略，巩固提升市场竞争能力。公司安全运营业务自2018年开始开展，以智慧城市业务破局，为智慧城市建设提供全套打包的安全服务，增强了公司在区域的穿刺能力，提高和巩固和公司的市场地位和竞争能力。目前公司已基本形成以北京、程度、广州、杭州四个运营业务支撑中心以及二十多个城市级运营中心的运营体系，19年上半年新增运营业务订单超过亿元。

绿盟科技：国资入股拉动政府端业务，股权结构改善重回经营正轨

公司第一大股东变更为中电科，国资入股有望持续拉动政府、军队端的订单需求提

升。2019年2月，公司公告称，股东IAB将转让约1514万股股份至中电基金、5598万股至网安基金，合计占公司总股本的8.8826%，同时股东联想投资将转让约3996万股公司股份给中电基金，占公司总股本的4.9902%。同年7月，电科投资通过二级市场买入公司股份约1305万股，占公司总股本的1.6292%，通过上述一系列变动，电科投资及其一致行动人中电基金、网安基金（均为中国电科CETC所属）合计持有公司15.5%的总股本，成为公司第一大股东，拉动公司在政府、军队侧的订单需求，2019年上半年，公司政府、事业单位及其他收入增速达到31.92%，超过其他行业，与去年年底增速相比实现大翻转。

图表 42：细分领域增速恢复，综合综合稳健



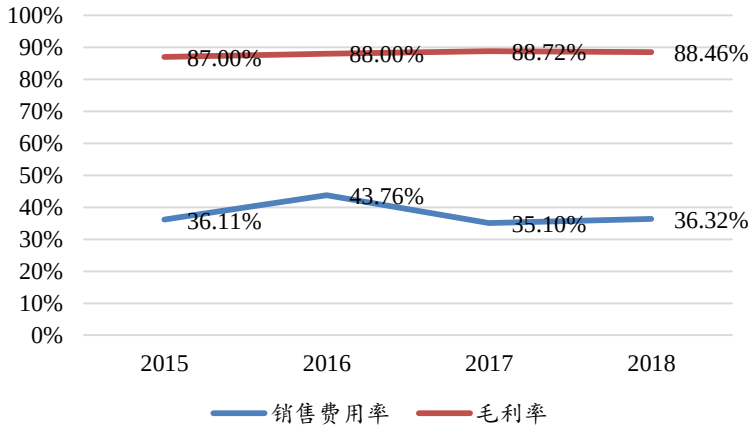
资料来源：WIND，太平洋证券整理

公司股权问题得到有效纾解，重回正轨专注业务发展。公司负责人沈继业通过自身持股及其控制的亿安宝诚合计持有公司15.46%的股权，成为公司第二大股东，外部股东IAB及联想投资不再持有公司股权，有利于优化公司内部经营管理和决策效率，公司后续将专注于公司业务经营和发展，涅槃重生。

深信服：全面进击信息安全市场，超融合领域持续领先

公司全面进入信息安全市场，依托强大渠道稳步推进。目前公司信息安全业务主要包括上网行为管理、下一代防火墙、VPN、应用交付、SD-WAN、安全态势感知、终端安全、云安全资源池、信息安全等级保护、安全即服务等产品及服务，其中多项产品多次入围Gartner魔力象限。公司销售以渠道营销模式为主，销售费用率常年保持在35%以上，依托深厚强大的渠道能力，公司安全业务毛利率始终居于行业高位。目前公司在保持渠道优势的前提下，正积极开拓直销端，向信息安全市场全面进击。

图表 43：公司销售费用率和安全业务毛利率领先行业水平



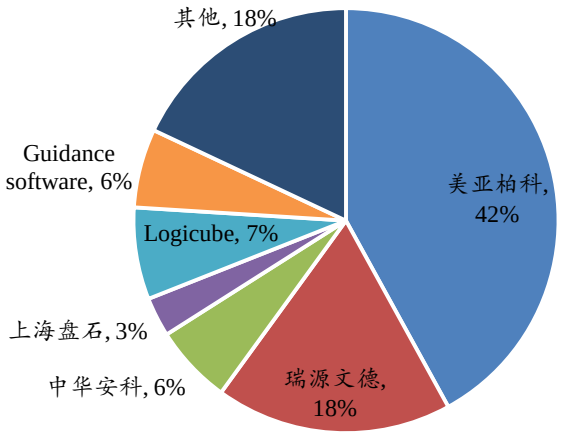
资料来源：WIND，太平洋证券整理

公司在超融合领域保持领先，桌面云、云管理平台等产品发展态势良好。公司自2012年进入云计算业务，积极布局桌面云、超融合、私有云等领域。根据IDC发布的报告，2018年超融合软件市场公司占有率排在第二位，占比17.4%，超融合软硬件总体市场公司稳居前三，占比15.5%。截止2019年，公司超融合用户超过4万家，超融合一体机已累计交付60000C，桌面云、云管平台等有序发展，根据IDC统计，2018年公司桌面云以15.9%的占比排在全国第二位，全年实现53.5%的高增速。

美亚柏科：电子取证业务迎来拐点，公安大数据平台维持高景气度

公司是电子取证领域龙头，组织机构变革完成取证业务有望迎来增长拐点。公司在电子取证业务领域保持绝对领先地位，市场占有率为42%，远远领先行业内其他竞争对手。目前随着组织机构变革的完成，公司传统网安业务逐渐复苏，有望在今年下半年迎来订单和业绩上的双拐点。同时公司积极拓展下游客户，客户结构更加丰富，突破传统网安至刑侦、经侦等警种，跨行业至监察委、税务和军工等，带来业绩上的增益。

图表 44：美亚柏科在电子取证业务保持绝对龙头地位



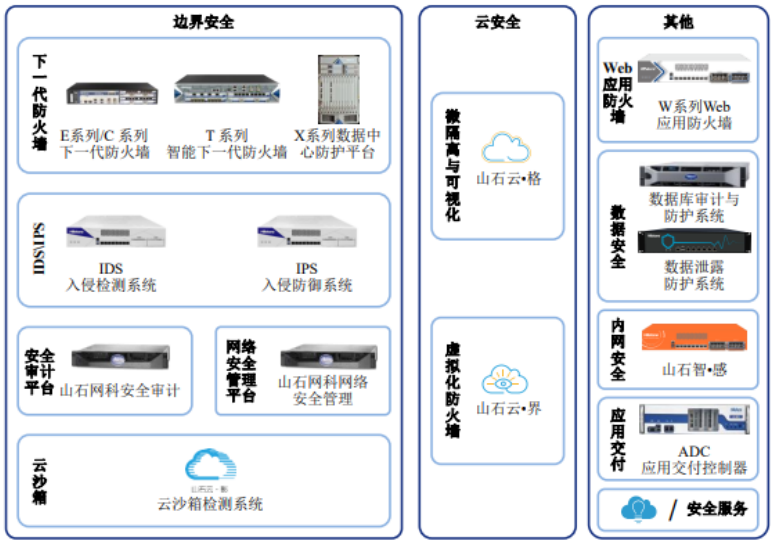
资料来源：中国产业信息网，太平洋证券整理

公安大数据平台建设保持高景气度。公安大数据平台主要用于打破各警种信息化建设的烟囱，实现网络数据、视频数据和传统网安数据的深度融合，提高公安工作的整体效率。公安大数据业务在过去2年保持着77%的复合增速，2018年实现营业收入4.96亿元，逐渐成长为公司另一大业绩支撑。伴随着更多城市公安大数据平台的建设，以及后续网络数据扩容上的需求，公安大数据平台业务仍将保持高速增长。

山石网科：成长性佳，科创板上市募资增强技术实力

目前公司产品主要包含边界安全和云安全产品，其中边界安全占到公司主营业务的90%以上。公司具备一定自主研发实力，公司下一代防火墙在最高吞吐量、新建连接数量、 并发连接数量等方面领先国内外绝大部分安全厂商。同时，公司连续五年入选 Gartner “企业级防火墙魔力象限”和“UTM 魔力象限” 的“特定领域者”象限，连续两年入选 Gartner “IDPS 魔力象限”的“特定领域者”象限。根据IDC数据，2018年公司统一威胁管理UTM市场份额排在第四位。云安全领域，公司在2013年成为VMware的合作伙伴，2018年获得VMware公司“VMware Ready”认证，自主研发的“山石 云•界” 在AWS、Azure、阿里云、腾讯云、华为云等公有云市场上架，并获得了较高部署量排名。

图表 45：山石网科主要产品和服务



资料来源：招股说明书，太平洋证券整理

公司本次登陆科创板，拟募集8.94亿元，用于网络安全产品线拓展升级、高性能云计算安全产品研发和营销网络的建设上，将进一步增强公司的技术实力和营销能力。

图表 46：山石网科募集资金用途

项目名称	投入金额（万元）	占比
网络安全产品线拓展升级项目	44,405.81	49.65%
高性能云计算安全产品研发项目	28,622.74	32.00%
营销网络及服务体系建设项目	16,411.81	18.35%

资料来源：招股说明书，太平洋证券整理

风险提示

军队业务订单增长存在不确定性；安全运营中心业务竞争者增加，头部竞争格局激烈；等保 2.0 的实质性推进过程中对历史市占率的颠覆等。

投资评级说明

1、行业评级

看好：我们预计未来 6 个月内，行业整体回报高于市场整体水平 5%以上；

中性：我们预计未来 6 个月内，行业整体回报介于市场整体水平－5%与 5%之间；

看淡：我们预计未来 6 个月内，行业整体回报低于市场整体水平 5%以下。

2、公司评级

买入：我们预计未来 6 个月内，个股相对大盘涨幅在 15%以上；

增持：我们预计未来 6 个月内，个股相对大盘涨幅介于 5%与 15%之间；

持有：我们预计未来 6 个月内，个股相对大盘涨幅介于-5%与 5%之间；

减持：我们预计未来 6 个月内，个股相对大盘涨幅介于-5%与-15%之间；

销 售 团 队

职务	姓名	手机	邮箱
华北销售总监	王均丽	13910596682	wangjl@tpyzq.com
华北销售	成小勇	18519233712	chengxy@tpyzq.com
华北销售	孟超	13581759033	mengchao@tpyzq.com
华北销售	付禹璇	18515222902	fuyx@tpyzq.com
华北销售	韦珂嘉	13701050353	weikj@tpyzq.com
华东销售副总监	陈辉弥	13564966111	chenhm@tpyzq.com
华东销售	李洋洋	18616341722	liyangyang@tpyzq.com
华东销售	杨海萍	17717461796	yanghp@tpyzq.com
华东销售	梁金萍	15999569845	liangjp@tpyzq.com
华东销售	杨晶	18616086730	yangjinga@tpyzq.com
华东销售	秦娟娟	18717767929	qinjj@tpyzq.com
华东销售	王玉琪	17321189545	wangyq@tpyzq.com
华东销售	慈晓聪	18621268712	cixc@tpyzq.com
华南销售总监	张茜萍	13923766888	zhangqp@tpyzq.com
华南销售	查方龙	18520786811	zhafl@tpyzq.com
华南销售	胡博涵	18566223256	hubh@tpyzq.com
华南销售	陈婷婷	18566247668	chentt@tpyzq.com

华南销售	张卓粤	13554982912	zhangzy@tpyzq.com
华南销售	张文婷	18820150251	zhangwt@tpyzq.com

太平洋证券
PACIFIC SECURITIES

研究院

中国北京 100044

北京市西城区北展北街九号

华远·企业号 D 座

电话：（8610)88321761

传真：（8610）88321566

重要声明

太平洋证券股份有限公司具有证券投资咨询业务资格，经营证券业务许可证编号 13480000。

本报告信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证。负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。报告中的内容和意见仅供参考，并不构成对所述证券买卖的出价或询价。我公司及其雇员对使用本报告及其内容所引发的任何直接或间接损失概不负责。我公司或关联机构可能会持有报告中所提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行业务服务。