渤海证券 BOHAI SECURITIES 研究所

多因素共振，网络安全前景广阔

——中小盘行业深度研究报告

分析师：徐中华 SAC NO：S1150518070003 2019 年 4 月 24 日

证券分析师
徐中华
010-68104898
xuzh@bhzq.com

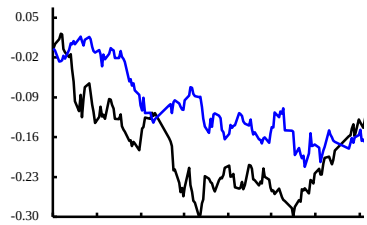
子行业评级

中小盘市值	看好

重点品种推荐

中孚信息	买入
启明星辰	买入
美亚柏科	买入

最近一年行业相对走势



投资要点：

- **网络安全行业成长快，市场规模持续扩大**

根据 Gartner 的统计数据，2017 年全球网络安全产业规模达到 989.86 亿美元，较 2016 年增长 7.9%，预计到 2018 年市场规模可增长至 1060 亿美元。与全球网络安全市场相比，中国的网络安全行业起步较晚，市场规模较小，但发展速度较快。根据赛迪顾问的测算，2018 年我国网络安全市场规模为 495.2 亿元，同比增长 20.9%，远高于全球市场的平均增速。同时，随着各项网络安全政策法规的逐步完善，以及国家和企业组织对网络安全的重视程度不断提升，对网络安全的投资逐渐增加，赛迪顾问预计未来三年我国网络安全市场仍将会保持 20%以上的高速增长，到 2021 年市场规模可超过 900 亿元。

- **多因素叠加，网络安全行业前景广阔**

网络安全行业的快速发展主要源于：1）安全威胁不断增加，根据国家互联网应急中心的数据，2017 年 CNCERT/CC 通过自主捕获和厂商交换发现的移动互联网恶意程序数量已经达到 253 万个，较 2016 年增长了 23.4%，2017 年，国家信息安全漏洞共享平台 CNVD 收录的安全漏洞数量再次出现爆发式增长，达到 15955 个，比 2016 年增加了 47.4%。2）信息技术持续进步带来的行业创新，网络安全行业的发展与信息技术的快速创新紧密相关。随着云计算、大数据、物联网、5G、人工智能等新兴信息技术的快速进步，网络安全防护技术也处于不断迭代更新的进程中。3）政策支持力度持续增强，2017 年开始实施的《网络安全法》，，它的实施正式将网络安全上升到国家安全的战略高度，使网络安全成为国家安全观的重要组成部分。而伴随着《网络安全法》的实施，我国新一代的等级保护制度也正在逐步完善，22018 年，公安部发布《网络安全等级保护条例(征求意见稿)》，意味着等保 2.0 体系的基本确定，为我国在云时代下的网络安全指明了发展方向。

- **投资建议**

随着信息技术的持续发展和自主可控需求的不断增强，网络安全行业的重要性也越来越突出。在互联网和移动互联网的不断发展，联网终端与系统数量持续增加，对于电子取证设备的需求和大数据分析产品的需求不断增加，在这个领域建议重点关注美亚柏科(300188)。在自主可控需求不断增加的基础上，对于安全保密产品的需求也随之增加，建议重点关注安全保密行业的领先企业中孚信息(300659)。网络安全行业快速发展，引发了对综合网络安全产品和安全服务的需求不断提升，在这个领域，建议重点关注启明星辰(002439)。

- **风险提示**

网络安全政策落地进展不及预期，技术进步不及预期，行业竞争加剧等。

目 录

图 目 录

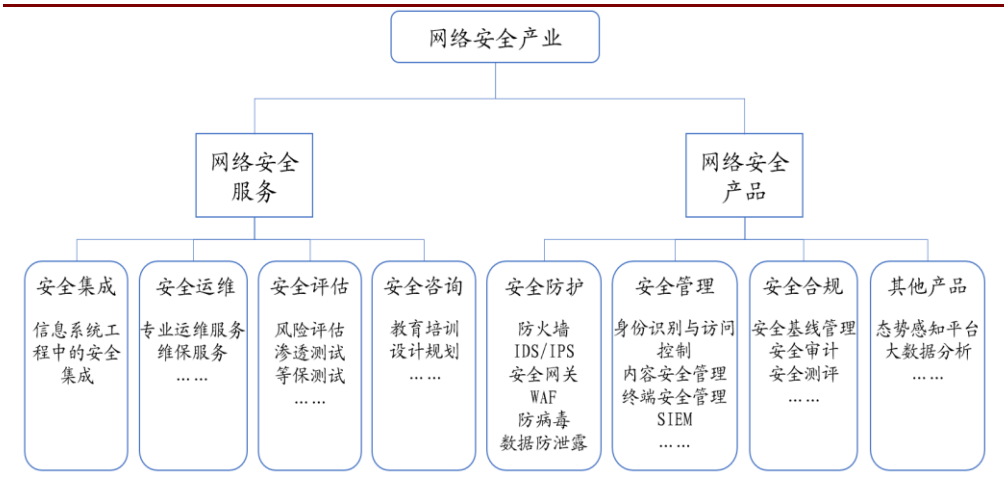
表 目 录

1.网络安全行业成长快，市场规模持续扩大

1.1 网络安全细分行业多，市场规模不断扩大

网络安全产业主要指防止网络中运行的数据信息遭到泄露、篡改、破坏，确保网络服务、系统正常运行等一系列保障网络运行的可靠性、安全性的产品和服务的集合。根据中国信通院在《网络安全产业白皮书(2017 年)》中给出的定义，网络安全市场按照主要功能及形态可分为安全产品市场和安全服务市场。其中安全产品领域又可细分为安全防护、安全管理、安全合规、其他安全产品四个类别。安全服务领域则主要包括安全集成、安全运维、安全评估和安全咨询四大类。

图 1：网络安全行业依据功能及形态分类



资料来源：中国信通院，渤海证券

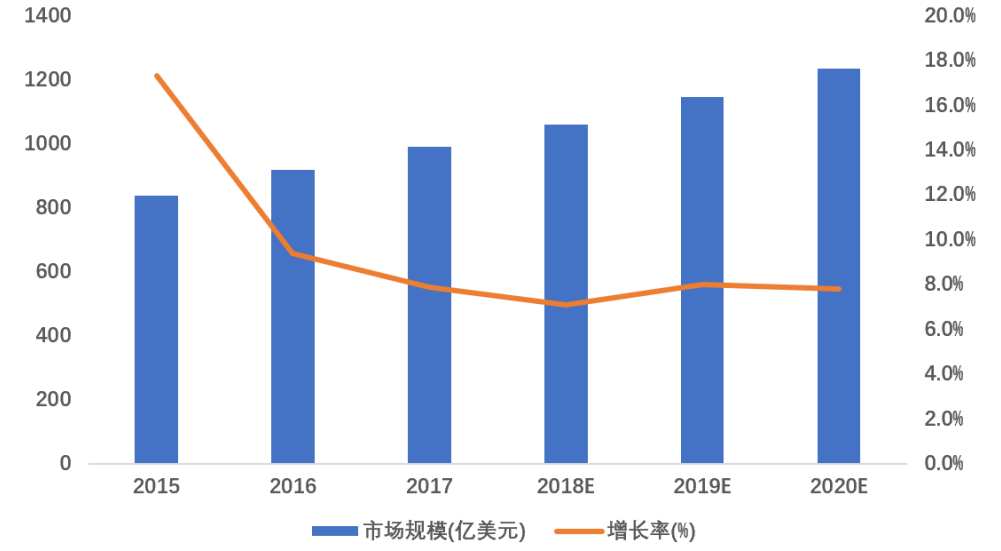
随着信息技术的快速发展，新技术与新产品层出不穷，网络安全行业也越来越呈现碎片化、复杂多样化的特征。2019 年 1 月，安全牛发布了最新的中国网络安全行业全景图，从安全防护技术的不同应用领域的角度对当前我国网络安全行业进行了划分。其中，工业互联网安全、态势感知、渗透测试和安全运维领域均有超过 20 家安全企业；物联网安全、云安全和安全智能领域逐步成为安全厂商重点关注的新兴领域。

图 2：我国网络安全行业全景图

资料来源：安全牛，渤海证券

近年来，随着以大数据、云计算、人工智能为代表的新一代信息技术的兴起，网络安全事故也随着网络空间的延伸和复杂化变得愈发多样化，并由此带动了网络安全行业的飞速发展。根据咨询机构 Gartner 的统计数据，2017 年全球网络安全产业规模达到 989.86 亿美元，较 2016 年增长 7.9%，预计到 2018 年市场规模可增长至 1060 亿美元。

图 3：全球网络安全市场规模及增长情况

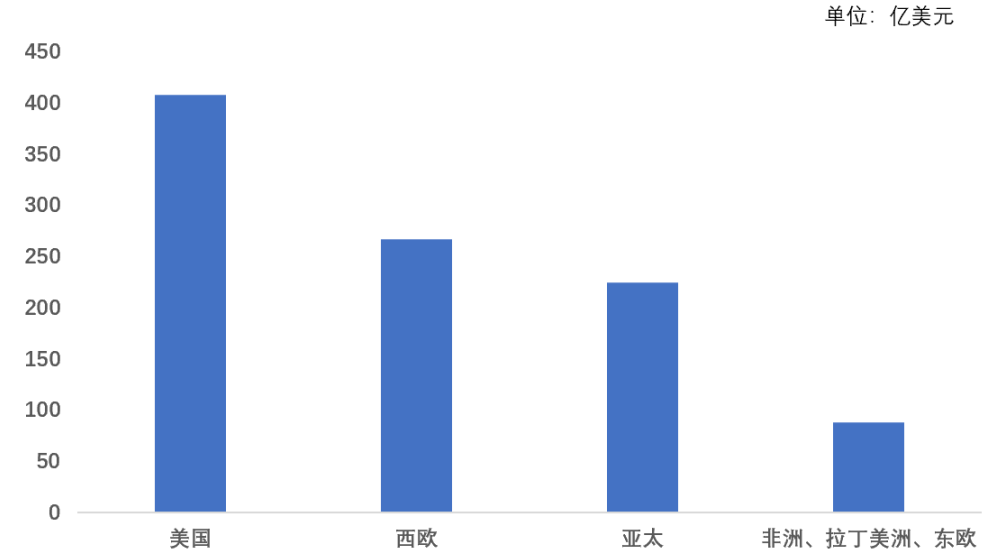


资料来源：Gartner，渤海证券

分不同区域来看，美国和加拿大所在的北美地区占据了全球网络安全市场最大的份额。该地区 2017 年市场规模相比 2016 年增长 9.24%，达到 408.76 亿美元，占据了全球市场 41.29%的份额。西欧地区市场份额位列第二，市场规模合计为 267.29 亿美元。日本、中国等 10 个亚太国家市场规模合计 225.08 亿美元，占比

22.74%，但增长速度 9.53%位列第一。总体来看，北美、西欧、亚太三个地区市场份额合计超过 90%，亚太地区，尤其是中国，网络安全行业增长较快。

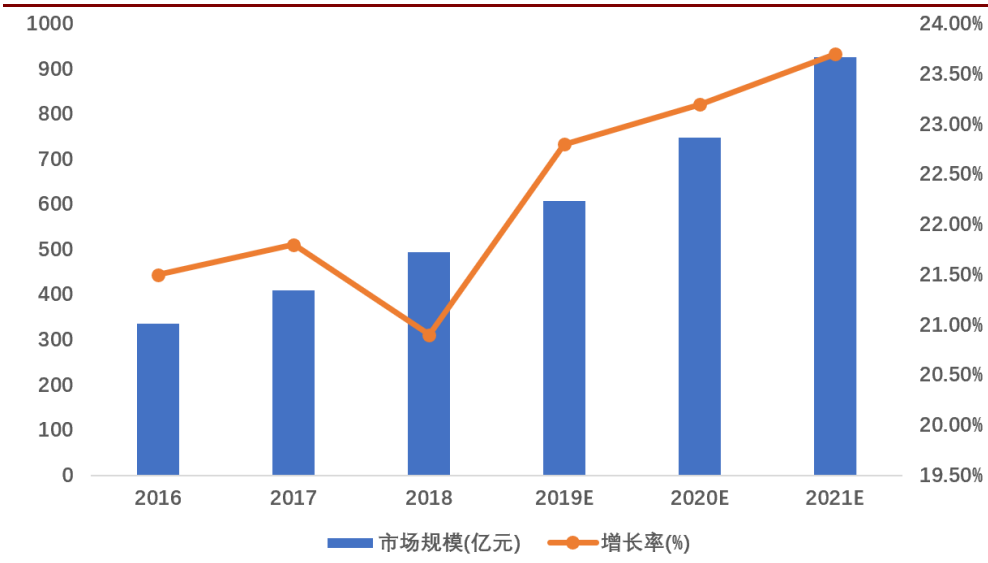
图 4：全球网络安全行业不同区域市场规模



资料来源：Gartner，中国信通院，渤海证券

与全球网络安全市场相比，中国的网络安全行业起步较晚，市场规模较小，但发展速度较快。根据赛迪顾问的测算，2018 年我国网络安全市场规模为 495.2 亿元，同比增长 20.9%，远高于全球市场的平均增速。同时，随着各项网络安全政策法规的逐步完善，以及国家和企业组织对网络安全的重视程度不断提升，对网络安全的投资逐渐增加，赛迪顾问预计未来三年我国网络安全市场仍将会保持 20%以上的高速增长，到 2021 年市场规模可超过 900 亿元。

图 5：我国网络安全市场规模及增长率

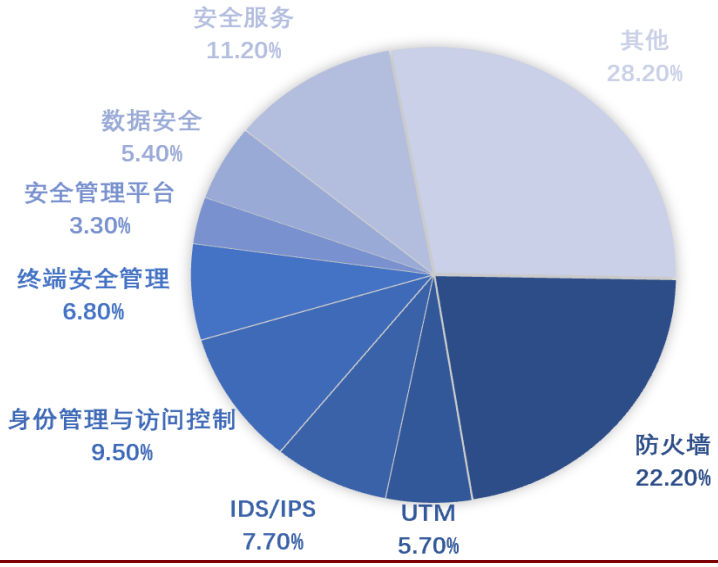


资料来源：赛迪顾问，渤海证券

1.2 传统安全产品占比高，市场集中度低

在市场结构方面，相比国外安全服务占比较高的局面，我国传统的安全防护类产品在市场中仍然占据主导，而又由于安全产品领域产品线较多，且传统经营模式主要以单一的产品采购为主，因此我国安全产品市场总体上格局比较分散。根据智研咨询的报告，当前市场中占比最大的是防火墙类产品，占整个网络安全市场规模的 22.2%；其次是身份管理与访问控制类产品，在网络安全市场中占比为 9.5%。总体来看，以大数据和人工智能技术为基础的新一代网络安全产品所占份额较低。

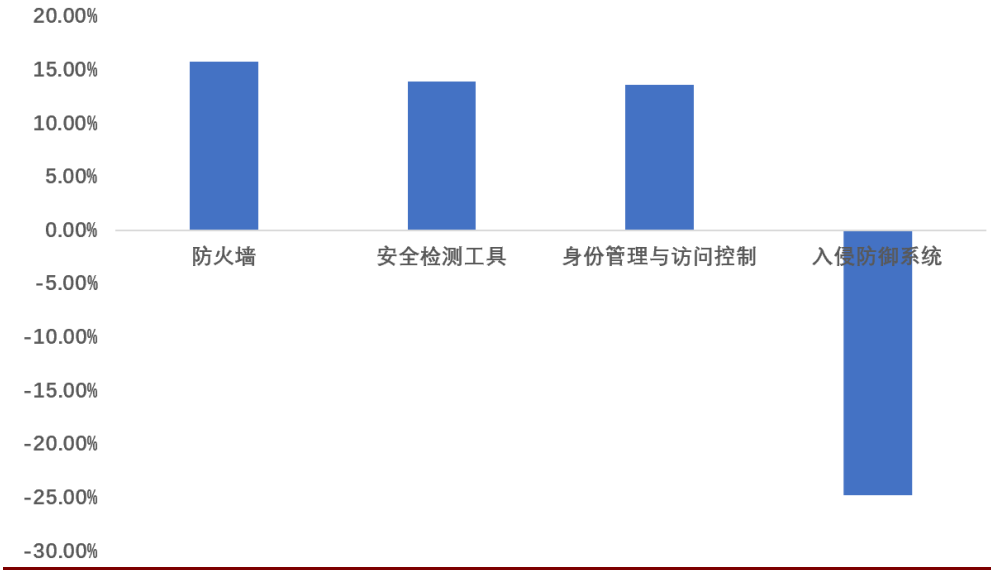
图 6：2017 年我国安全产品市场份额



资料来源：智研咨询，渤海证券

根据 Gartner 的统计，2017 年全球安全产品细分市场中，防火墙、安全检测工具和身份管理与访问控制产品增速较快。其中，防火墙市场增速达到 15.8%，核心推动因素为数据中心等大规模网络的部署、大型企业集中化管理和传统防火墙升级。安全检测工具增长 13.9%，企业内部安全事故频发引发了企业对内部风险排查的强烈需求，同时与人工智能结合的智能化安全检测技术也推动安全检测工具迅速增长。

图 7：2017 年全球安全产品细分市场增长率



资料来源：Gartner，渤海证券

竞争格局方面，我国网络安全市场集中度较低，领军企业规模优势尚不明显。根据中国网络安全产业联盟发布的《2018 年中国网络安全产业报告》，我国网络安全行业集中度较低，CR1<10%，CR5<30%，CR10<50%。国内多数安全厂商还处于市场开拓时期，从产品研发到渠道营销暂未形成具有规模优势的龙头企业。这主要是因为传统的网络安全服务是以产品分散采购为主，各产品之间缺乏整体性，企业只是单纯的负责单一类型产品的销售以及驻场式的被动安全服务，并未考虑整体化的安全运维。

图 8：2018 年我国网络安全市场集中度

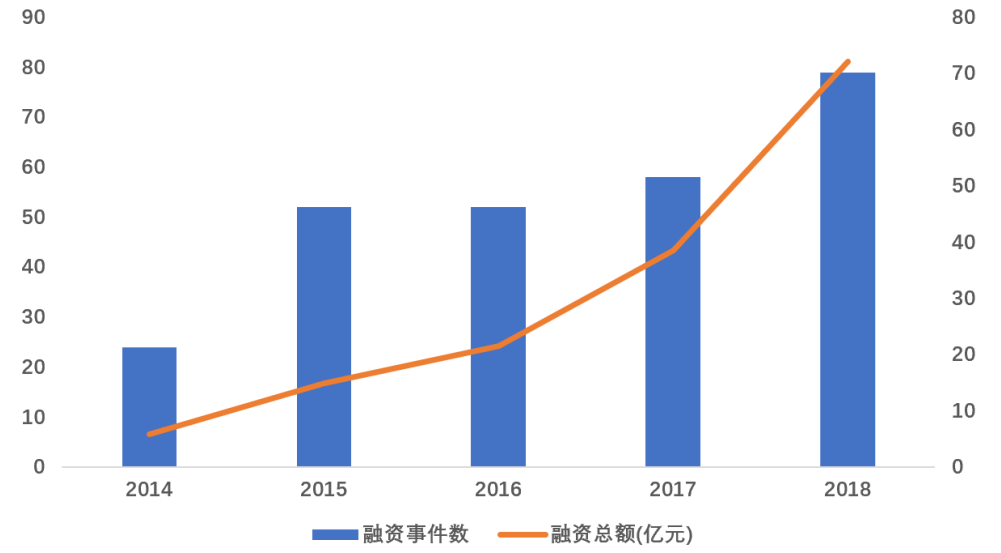
资料来源：中国网络安全产业联盟，数说安全，渤海证券

从市场集中度和行业内企业规模可以看出，我国网络安全行业还处于快速成长期，行业内竞争激烈，产品和服务高度分散化。

1.3 一级市场活跃，资本助力行业快速发展

资本市场对于网络安全领域的关注也逐渐提高，网络安全企业融资数量和金额不断提高。根据中国信通院的统计数据，截至 2018 年 4 月，国内已获得融资网络安全企业已达到 135 家，参与网络安全领域投资企业 100 家。同时赛迪顾问发表的报告显示，2018 年我国网络安全企业融资事件共发生 79 起，融资金额达 72.1 亿元，相比 2016 年融资金额增长 86.78%；相比 2014 年，2018 年发生的融资事件是当年的 3.29 倍，而融资金额更是增长了 11.43 倍，年复合增长率为 87.77%。

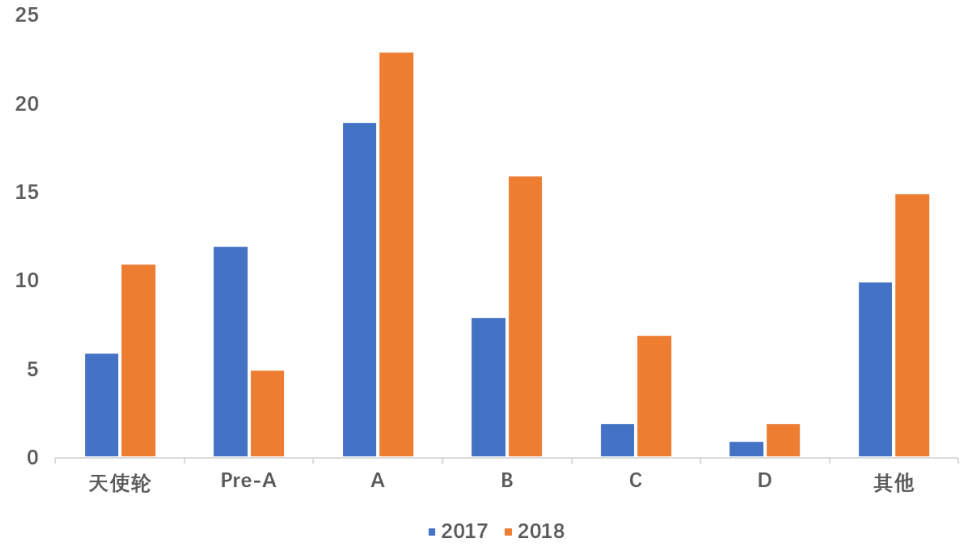
图 9：我国网络安全领域融资数量和金额增长情况



资料来源：赛迪顾问，渤海证券

2018 年，一级市场针对网络安全企业的天使轮融资发生 11 起，A 轮融资发生 23 起。对初创期企业融资力度的加大显示出市场对网络安全行业前景的看好，对加速行业的规模扩张和技术进步起到较强的推动作用。

图 10：2017-2018 年我国网络安全行业融资轮次分布



资料来源：赛迪顾问，渤海证券

2018 年至 2019 年 3 月，我国一级市场发生的融资额在 1 亿以上或估值在 10 亿以上的安全企业进行的融资活动共计融资超过 30 亿元。融资企业重点技术领域集中在身份管理与访问控制、云安全、安全智能、数据安全、移动安全等新兴网络安全领域。

表 1：2018 年至今我国主要未上市网络安全企业融资情况

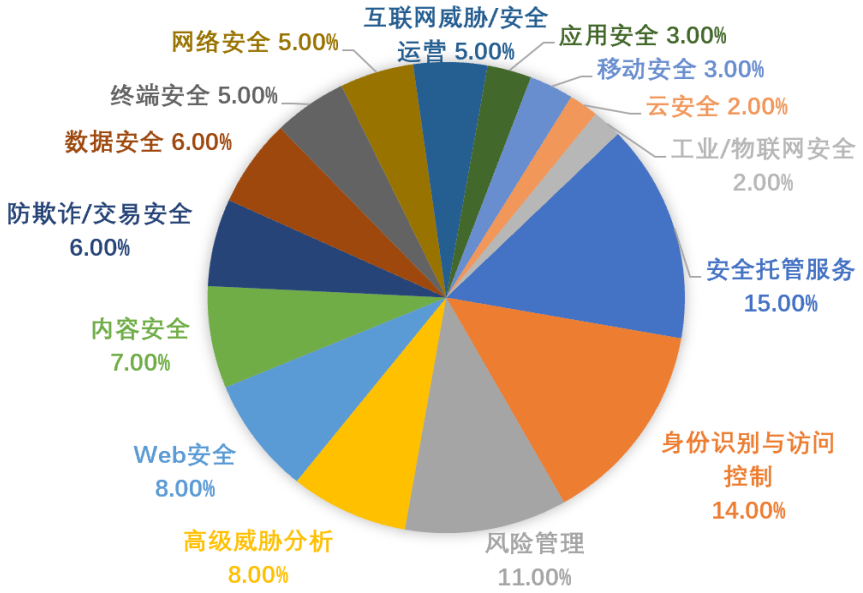
时间	融资企业	重点领域	融资轮次	金额	最新估值
2019.1.17	芯盾时代	身份管理与访问控制	C 轮	3 亿元	15 亿元
2019.1.7	360 企业安全	云安全、安全智能	B 轮	9 亿元	206.5 亿元
2019.1.3	漏洞盒子	安全服务	B+轮	1 亿元	5 亿元
2018.12.6	爱加密	移动安全	战略投资	数千万元	20 亿元
2018.11.28	360 企业安全	云安全、安全智能	Pre-B 轮	12.5 亿元	206.5 亿元
2018.11.3	安华金和	数据安全	C 轮	亿元及以上	5 亿元
2018.10.26	极御云安全	云安全	A 轮	2000 万美元	6.5 亿元
2018.10.15	指掌易科技	移动安全	B 轮	2 亿元	16 亿元
2018.10.12	高重科技	安全智能	A 轮	1 亿元	5 亿元
2018.6.19	Hillstone 山石网科	云安全	战略投资	未透露	39 亿元
2018.5.22	竹云科技	身份管理与访问控制	A+轮	数千万元	10 亿元
2018.2.26	青藤云安全	云安全	B 轮	2 亿元	10 亿元
2018.1.17	爱加密	移动安全	D 轮	未透露	20 亿元
20181.15	芯盾时代	身份管理与访问控制	B+轮	1.2 亿元	15 亿元

资料来源：IT 桔子，渤海证券

在全球市场上，网络安全行业的并购态势比较鲜明的反映出当前市场对安全领域的关注重点。从并购的技术领域来看，安全服务、身份识别与访问控制成为最热

门的并购选择，发生的并购数量分别占据当年并购总数的 15%和 14%。

图 11：2017 年全球网络安全行业并购领域分布



资料来源：Momentum Cyber，中国信通院，渤海证券

根据中国信通院的统计，2017 年至 2018 年 9 月，国外共有 5 家网络安全企业进行 IPO，其技术重点均在身份管理与访问控制、云安全和风险管理领域。

表 2：2017-2018 年 9 月国际网络安全企业 IPO 情况

时间	企业	重点领域	募集资金
2017.4	Okta	身份管理与访问控制	1.74 亿美元
2017.10	Forescout	身份管理与访问控制	1.08 亿美元
2017.11	SailPoint	身份管理与访问控制	1.6 亿美元
2018.3	Zscaler	云安全	1.79 亿美元
2018.7	Tenable	风险管理	2.33 亿美元

资料来源：中国信通院，渤海证券

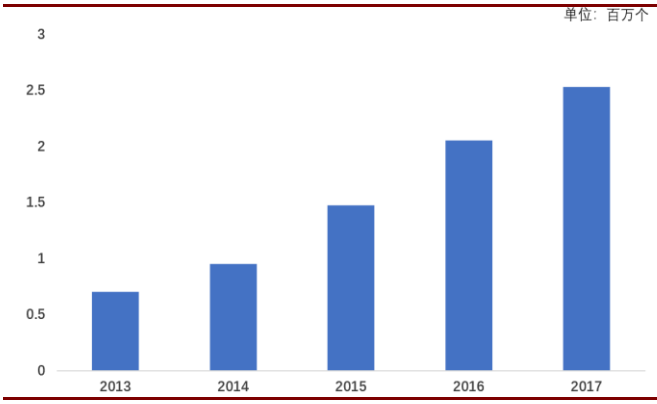
从国内外投资人对网络安全企业的投资选择上可以看出，受云计算、大数据、人工智能、移动互联网、工业互联网的影响而兴起的网络安全新兴领域成为资本市场关注的焦点，在资本推动下，或将迎来较快的发展。

2.多因素叠加，网络安全行业前景广阔

2.1 网络安全事故频发，安全威胁不断增加

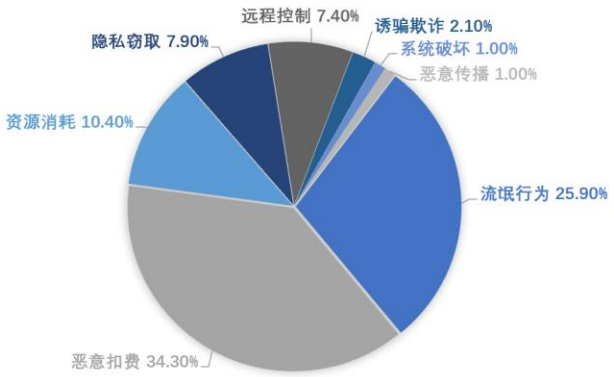
近几年，随着新一代信息技术的快速发展，围绕网络和数据的服务与应用呈爆发式增长，但与之相关的各种网络风险和问题也迅速增多，从传统网络病毒到各种新型攻击模式，各种恶意攻击层出不穷。根据国家互联网应急中心的数据，2017 年 CNCERT/CC 通过自主捕获和厂商交换发现的移动互联网恶意程序数量已经达到 253 万个，较 2016 年增长了 23.4%。具体分析这些恶意程序的恶意行为可以发现，占比最高的三类恶意行为是流氓行为、恶意扣费、资源消耗，分别占比 35.9%、34.3%和 10.4%。显然，随着移动互联网的飞速发展，我国在移动端面临的网络威胁愈发严峻。

图 12：2013-2017 年我国捕获的移动互联网恶意程序



资料来源：CNCERT/CC，渤海证券

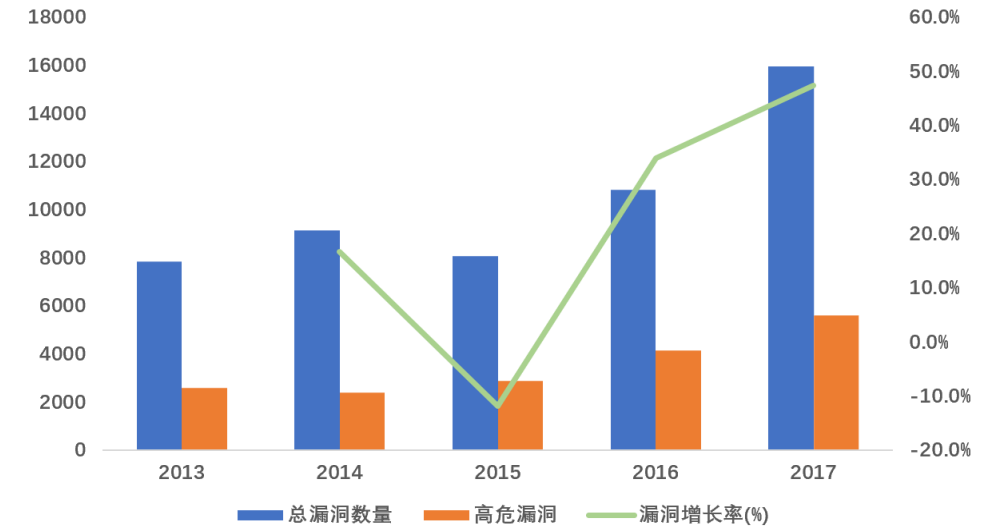
图 13：2017 年移动互联网恶意程序行为分类



资料来源：CNCERT/CC，渤海证券

互联网的发展、网络空间的不断深化，一方面在拓展虚拟互联边界的同时，另一方面也增加了网络漏洞出现的概率。2017 年，国家信息安全漏洞共享平台 CNVD 收录的安全漏洞数量再次出现爆发式增长，达到 15955 个，比 2016 年增加了 47.4%。

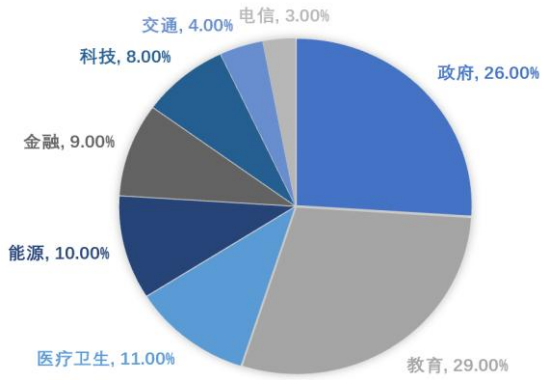
图 14：2013-2017 年我国收录的安全漏洞数量及增长情况



资料来源：CNCERT/CC，渤海证券

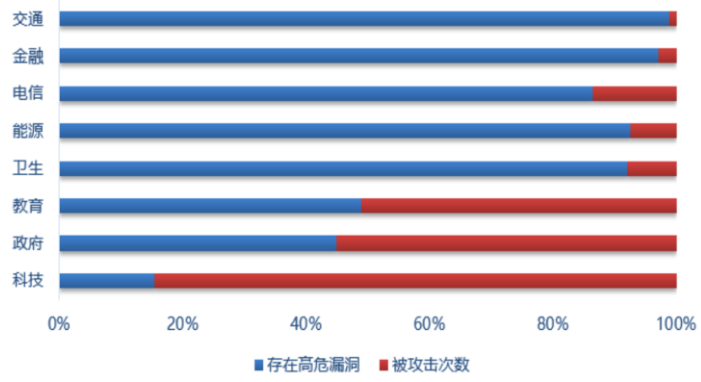
在操作系统漏洞方面，腾讯安全对 2018 年的 Windows 平台漏洞进行了收录和分析，发现 2018 年 Windows 操作系统的漏洞提交数量相较过往三年同比上升最高超过 40%，创历史新高。在 Windows 漏洞分布行业方面，教育、政府、医疗卫生是占比最高的三个行业。其中教育、政府领域因其存在大量高危漏洞而遭受了较多的攻击，但是科技行业在存在高危漏洞相对较少的情况下却遭受了最高的攻击量，说明对科技行业的重要机密窃取往往是攻击者的首要攻击目的。

图 15：2018 年 Windows 高危漏洞行业分布



资料来源：腾讯安全，渤海证券

图 16：2018 年各行业存在高危漏洞与被攻击次数对比



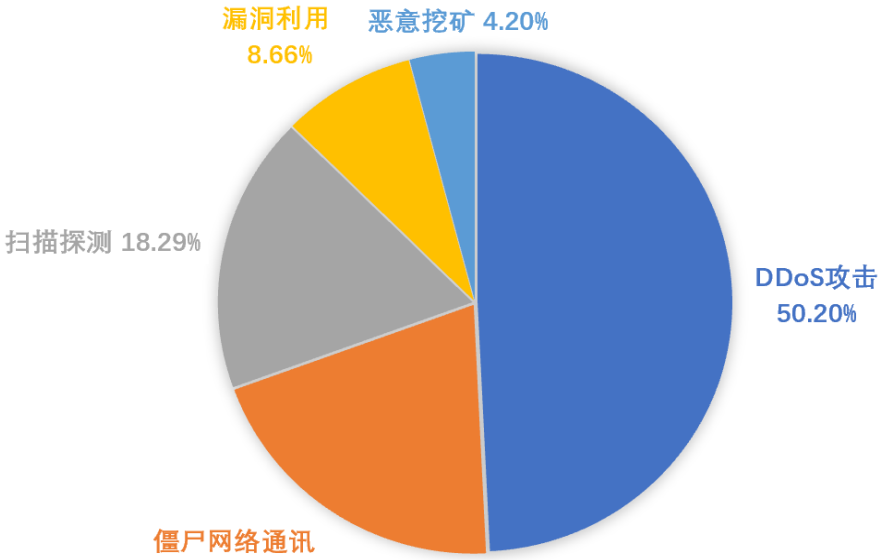
资料来源：腾讯安全，渤海证券

在 DDoS 攻击方面，根据绿盟科技的监测数据，其 2018 年共监控到 DDoS 攻击次数为 14.8 万次，攻击总流量 64.31 万 TB，攻击的平均峰值达到了 42.8Gbps，在 2018 下半年平均峰值甚至达到了 67Gbps。和 2017 年相比，攻击总流量虽然没有显著变化，但平均攻击峰值却增加了 2 倍有余。

同时 DDoS 攻击对我国物联网设备的正常运行也造成了很大的负面影响。据绿盟科技统计，我国物联网设备的异常行为，有一半是 DDoS 攻击造成的，僵尸网络

通讯和扫描探测分别造成了 20.63%和 18.29%的异常行为。

图 17：2018 年我国异常物联网设备行为占比



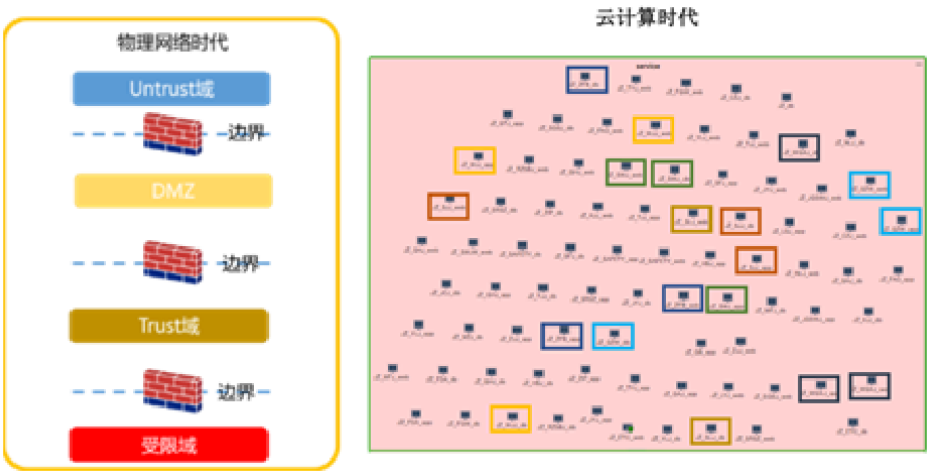
资料来源：绿盟科技，渤海证券

2.2 信息技术持续进步，网络安全行业不断创新

网络安全行业的发展与信息技术的快速创新紧密相关。随着云计算、大数据、物联网、5G、人工智能等新兴信息技术的快速进步，网络安全防护技术也处于不断迭代更新的进程中。

传统的安全防护思想是基于“网络边界”而将企业或组织的内部网络与外部互联网进行隔离，隔离完成后便默认内网是安全可信的，在边界内部的事物基本上可以畅通无阻的运行，拥有大部分的访问权限。但云计算的出现打破了企业网络边界的概念，呈现出与传统网络截然不同的运行方式：1）安全域放大。云计算环境下，虚拟化技术的运用会让一个由几台物理服务器划分出的传统安全域被放大几十倍；2）网络边界不明显。云计算环境下虚机可以在不同物理服务器上迁移，这一方面提高了整个系统的业务持续性，却也对传统的按照固定物理边界配置安全策略的模式形成了挑战；3）云内不可视。同一物理服务器上，同一虚拟网络连接的虚拟服务器之间的通信流量会直接通过服务器上的虚拟交换机完成转发，流量不会经过物理服务器之间的物理交换机。4）数据量十分巨大。虚拟化技术会将一个普通的数据中心的工作量几十倍的放大，如果在云内出现攻击行为，定位问题、制定策略、实施具体配置等措施的复杂度都会大量增加。

图 18：物联网时代和云计算时代网络安全域划分对比



资料来源：Hillstone 山石网科，渤海证券

基于云计算时代复杂的网络安全环境，以“零信任”模型为核心思想的新一代身份管理与访问控制技术得到了迅速发展。在“零信任”框架下，企业打破了内网与外网的界限，不再使用边界防御策略，而是实行“全面身份化”——将企业中所有参与实体(包括人、设备、服务)以身份为中心进行动态访问控制。身份管理与访问控制技术作为基础性的安全技术，会逐渐由过去的单一、静态朝多维、动态方向发展，在云环境下会变得更加重要。

图 19：基于零信任模型的云身份认证

资料来源：九州云腾官网，渤海证券

2.3 网络安全重要性日益显现，相关政策法规密集出台

棱镜门事件后，我国对网络安全的重视迅速提升。2014 年，我国组建中央网络安全和信息化领导小组（后改名为中央网络安全和信息化委员会），开始从顶层层面对网络安全领域的发展建设进行规划设计。2016 年，我国颁布《网络安全法》，将其作为网络安全领域基础性、全局性的法律。它的实施正式将网络安全

上升到国家安全的战略高度，使网络安全成为国家安全观的重要组成部分。而伴随着《网络安全法》的实施，我国新一代的等级保护制度也正在逐步完善，2016 年 10 月公安部网络安全保卫局组织对原有的信息安全等级保护制度进行了修订，等保 2.0 体系开始建立；2018 年，公安部发布《网络安全等级保护条例(征求意见稿)》，意味着等保 2.0 体系的基本确定，为我国在云时代下的网络安全指明了发展方向。

表 3：2014 年以来我国在网络安全领域出台的重要政策与法律法规

时间	政策/部门	要点
2014 年 2 月	中央网络安全和信息化领导小组	国家主席习近平担任小组组长，强调信息化领导小组要统筹协调各个领域的网络安全和信息化重大问题，制定实施国家网络安全和信息化发展战略、宏观规划和重大政策；
2014 年 8 月	《关于加强电信和互联网行业网络安全工作的指导意见》	《意见》重点强调要提升网络安全保障能力，完善网络安全保障体系，提高网络基础设施和业务系统安全防护水平，增强网络安全技术能力；
2014 年 10 月	《关于进一步加强军队信息安全工作的意见》	《意见》强调要把信息安全工作作为网络强军的重要任务，要全面推开信息安全等级保护和风险评估，强力推进国产自主化建设应用，促进我军信息化建设科学、安全发展；
2016 年 11 月	《网络安全法》	《中华人民共和国网络安全法》正式发布，并于 2017 年 6 月 1 日开始实施。强调了金融、能源、交通、电子政务等行业在网络安全等级保护制度的建设，是我国第一部网络空间管理方面的基础性法律；
2016 年 12 月	《国家网络空间安全战略》	明确国家网络空间安全工作的战略任务是鉴定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、打击网络恐怖和违法犯罪、完善网络治理体系；
2016 年 12 月	《“十三五”国家信息化规划》	规划在提出打破信息壁垒，构建统一高效的国家数据资源体系的同时，还强调构建网络和信息安全检测预警、应急处置等保障体系，完善网络空间治理体系；
2017 年 1 月	《关于促进互联网健康有序发展的意见》	《意见》要求要加快完善市场准入制度，提升网络安全保障水平，维护用户合法权益、打击网络违法犯罪、增强网络管理能力，防范移动互联网安全风险；
2017 年 7 月	《关键信息基础设施安全保护条例(征求意见稿)》	明确要求地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价；
2017 年 8 月	《一流网络安全学院建设示范项目管理办法》	《办法》提出在 2017-2027 年实施一流网络安全学院建设示范项目，简称 4 至 6 所“国内公认、国际上具有影响力和知名度”的网络安全学院的目标；
2018 年 3 月	《关于推动资本市场服务网络强国建设的指导意见》	《意见》重点强调要推动网信事业和资本市场协调发展，保障国家网络安全和金融安全，促进网信和证券监督工作联动。
2018 年 6 月	《网络安全等级保护条例(征求意见稿)》	新条例将等保对象有原来的“信息系统”改为“网络和信息系统”，包括了云计算平台、大数据平台、移动互联、物联网和工业控制系统等，确保关键信息基础设施的安全。

资料来源：政府网站，渤海证券

《网络安全法》作为我国网络安全领域地位最高、最重要的基础性法律，对我国网络安全行业的健康有序发展具有重要促进作用，也奠定了网安行业在国家经济发展进程中的战略性地位。《网络安全法》共包括 7 章 79 条，核心思想是辅助构建一个规范的、“防御、控制与惩治”三位一体的网络安全架构。

随着 2017 年《网络安全法》的正式实施，相关的网络安全配套政策和安全标准也开始陆续发布，其中最重要的便是《关键信息基础设施安全保护条例(征求意见稿)》和《网络安全等级保护条例(征求意见稿)》。2018 年，公安部发布《网络安全等级保护条例(征求意见稿)》，意味着等保 2.0 体系基本确定。总体来看，等保 2.0 主要是在等保对象和技术要求两个方面发生了重大变化。

在等保对象上，随着网络环境更加复杂，等保 1.0 标准中提出的以基础信息网络和传统信息网络作为保护对象已经不能涵盖所有的重要网络系统。基于此，等保 2.0 中的等保对象范围得到全方位提升，除了传统的信息系统，还包括了大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等内容。

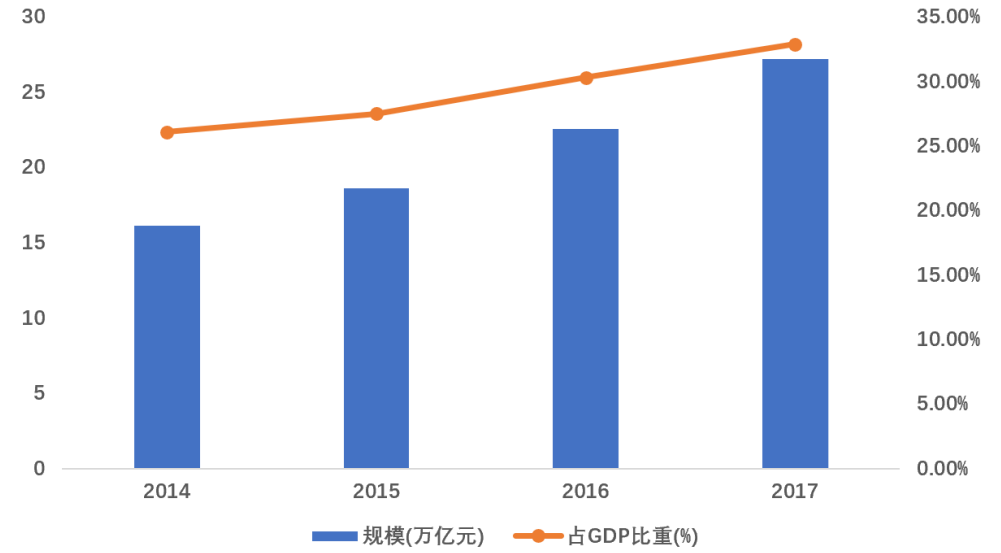
在技术要求方面，相比等保 1.0 标准，等保 2.0 将控制结构由原来的五个层面：物理安全、网络安全、主机安全、应用安全、数据安全，调整为四个部分：1）物理和环境安全；2）网络和通信安全；3）设备和计算安全；4）应用和数据安全。技术要求“从面到点”提出安全要求，“物理和环境安全”主要对机房设施提出要求，“网络和通信安全”主要对网络整体提出要求，“设备和计算安全”主要对构成节点（包括网络设备、安全设备、操作系统、数据库、中间件等）提出要求，“应用和数据安全”主要对业务应用和数据提出要求。

3.新兴领域快速成长，行业持续成长

3.1 数字经济蓬勃发展，云安全领域前景广

大数据的发展催生了经济数字化的浪潮，人们在生产生活中要面对和处理的数据规模与数据种类越来越庞大，其所承载的信息价值也越来越高，数据逐渐成为一种新兴的基础性资产，在经济活动中发挥至关重要的作用。根据中国信通院的报告，当前 G20 国家数字经济规模不断扩大，2017 年达到 26.17 万亿美元，同比增长 8.64%，其增速高于平均 GDP 增速约 2.12 个百分点，数字经济对各国经济发展的推动作用不断增强。中国数字经济占 GDP 的比重已经由 2014 年的 26.1%上升到 2017 年的 32.9%，数据在我国经济发展中的重要性越来越突出。

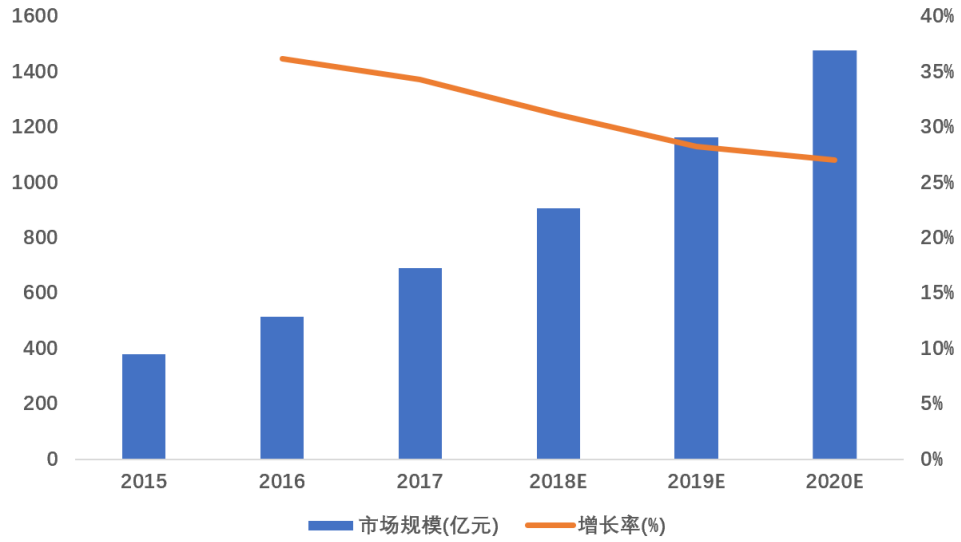
图 20：2014-2017 年中国数字经济规模及占 GDP 比重



资料来源：中国信通院，中商产业研究院，渤海证券

云计算是支撑数字经济发展的重要信息基础设施。中国信通院测算，2017 年我国云计算整体市场规模达 691.6 亿元，同比增速为 34.32%。其中，公有云市场规模达到 264.8 亿元，较 2016 年增长 55.7%；私有云市场规模达 426.8 亿元，较 2016 年增长 23.8%，预计未来几年，云计算市场将保持稳定增长，到 2021 年规模可达到 955.7 亿元。

图 21：中国云计算市场规模及增长率

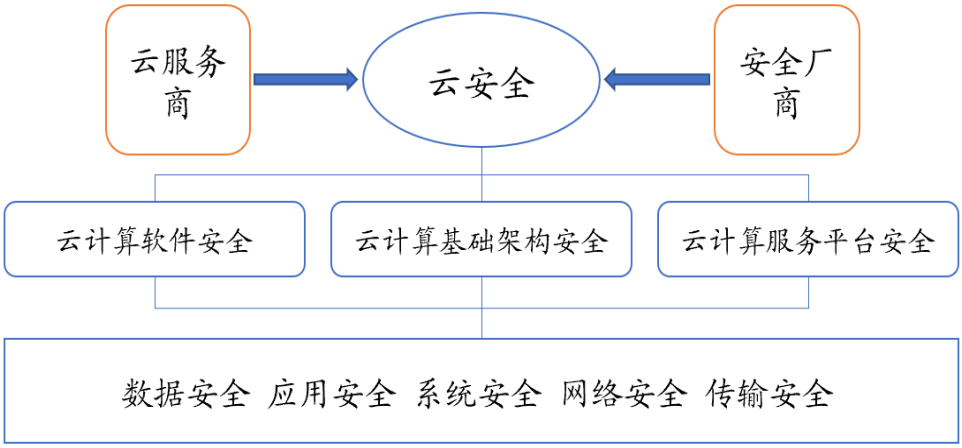


资料来源：中国信通院，渤海证券

随着云计算的普及，越来越多的企业组织选择将业务上云，云端上的数据资产的价值越来越大，云上数据泄露事件造成的成本损失也更加严重，不仅对普通企业的商业活动造成严重影响，部分事件更会威胁到国家安全。因此，云安全问题已成为政府、企业和社会各界广泛关注的焦点。

云安全行业具体来看包括了三大部分，即云计算软件安全、云计算基础架构安全和云计算服务平台安全，涉及数据、应用、系统、网络和传输等云计算平台各个方面。云安全市场的服务提供者主要是两类，第一类是云服务厂商，在为企业提供公有云服务的过程中同时提供云安全服务，另一类则为安全厂商，在私有云和混合云领域提供一揽子安全解决方案。

图 22：云安全市场概览

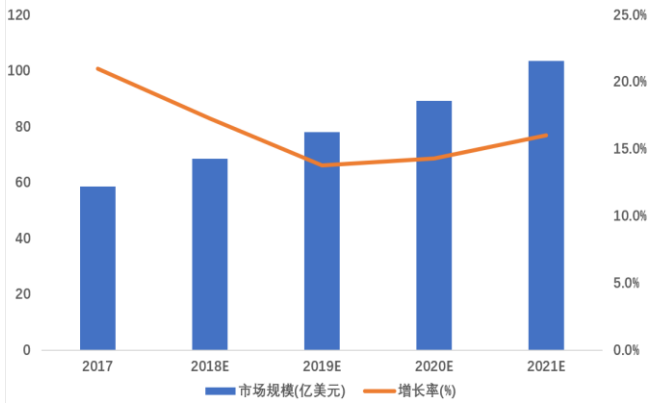


资料来源：前瞻产业研究院，渤海证券

在云计算产业的带动下，云安全市场飞速发展。据 Gartner 公司预计，随着越来

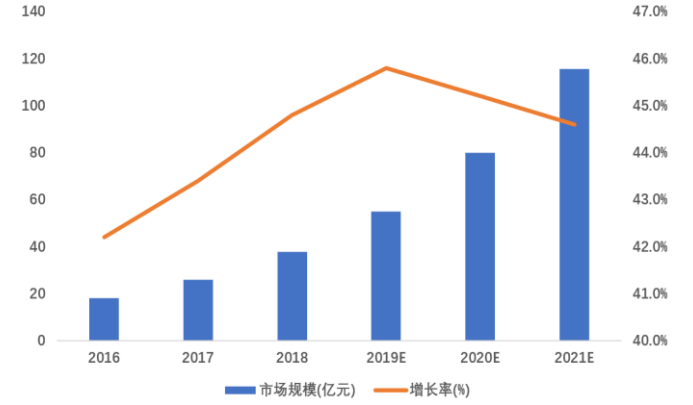
越多的中小企业使用云安全服务，全球云安全市场将会保持强劲增长。2017 年全球云安全市场规模为 58.51 亿美元，同比增长 21%。我国云安全市场成长更为迅速，据赛迪顾问发布的数据，2018 年我国云安全市场规模约为 37.8 亿元，相比 2017 年增长 44.8%，为全球平均增速的两倍以上，预计到 2021 年我国云安全市场规模达到 115.7 亿元。

图 23：全球云安全市场规模及增长率



资料来源：Gartner，前瞻产业研究院，渤海证券

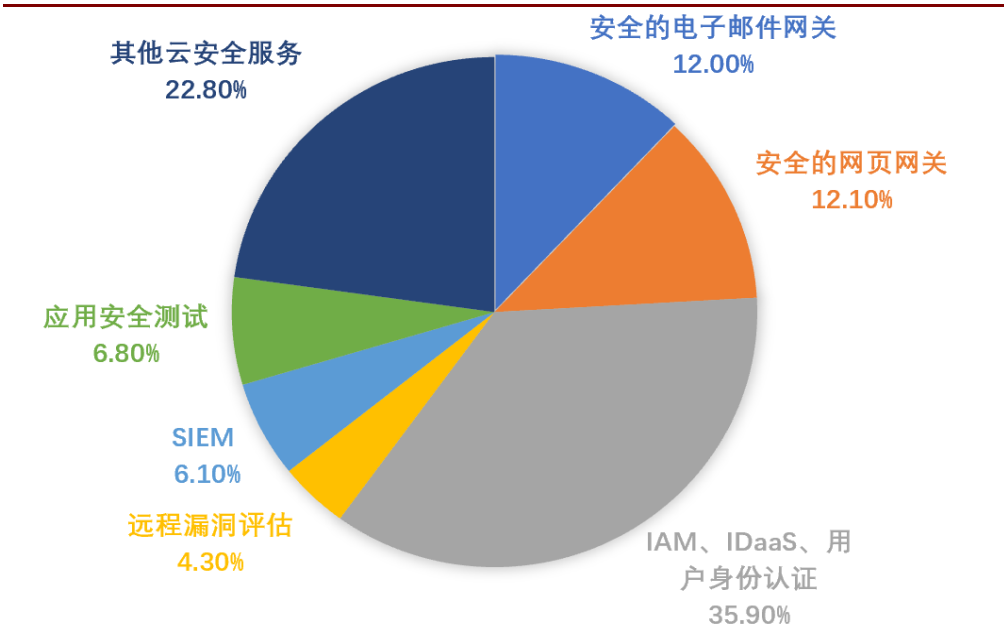
图 24：我国云安全市场规模及增长率



资料来源：赛迪顾问，渤海证券

根据 Gartner 对全球云安全市场的调查结果，2017 年全球云安全细分市场中，IAM、身份认证相关服务占比最大，占市场总额的 35.9%，同时该领域也是云安全市场中增长速度最快的，2017 年增长率为 27.3%。云计算的分布式运算和虚拟化的特点让企业对云身份管理和控制服务的需求日益增长，“全面身份化”将成为未来云时代下的网络安全防护的新特征。

图 25：2017 年全球云安全市场结构



资料来源：Gartner，前瞻产业研究院，渤海证券

根据安全牛发布的统计数据，我国云安全市场目前主要分为云抗 D、云 WAF、云身份管理、云基础架构安全和云主机安全五大细分领域，其中既有阿里云、腾讯云、华为云这种云服务厂商参与，也有众多的垂直安全厂商如青藤云安全、安恒信息等。

表 4：我国云安全领域细分市场及主要竞争厂商

云抗 D	云 WAF	云身份管理	云基础架构安全	云主机安全
阿里云	青松云安全	安恒信息	启明星辰	青藤云安全
腾讯云	安恒信息	芯盾时代	天融信	亚信安全
百度安全	新华三	炼石网络	亚信安全	志翔科技
电信云堤	阿里云	派拉软件	安恒信息	安全狗
知道创宇	腾讯云	创原天地	360 企业安全	360 企业安全
华为	华为		绿盟科技	
360 企业安全	百度安全		Hillstone 山石网科	

资料来源：安全牛，渤海证券

云服务商在发展云安全方面具有先天的资源和技术优势，依靠庞大的客户资源数据和自身在数据分析、AI、机器学习等技术领域的强大实力，可以为云租户提供云计算平台+云安全的组合服务模式，覆盖网络、主机、应用、业务、数据、管理等一系列安全产品与服务。我国云服务巨头，阿里、华为、腾讯等均建立了比较完备的云安全能力体系，比如在主机安全方面，阿里云推出“安骑士”产品，华为云推出“HSS”，腾讯云推出“云镜”，基本都包含安全配置核查、漏洞管理、入侵防护、基线检查等功能。

专业型安全厂商主要面向私有云和混合云，围绕云安全监测、防护、管理等需求，提供一揽子安全解决方案。

表 5：我国云安全领域主要安全厂商及其产品

公司	产品	主要功能
安恒信息	天池云安全运营平台	可提供监测、防御、审计、态势感知等安全能力；
亚信安全	服务器深度安全防护	旨在提升虚拟化和云项目投资收益率的同时简化安全操作；
Hillstone 山石网科	微隔离产品	使用创新的分布式网络侧微隔离，通过专利引流技术、虚机微隔离及可视化技术，提供包括流量及应用可视化，虚机之间威胁检测与隔离，网络应用审计等服务；
绿盟科技	云计算安全解决方案	把零散的虚拟化安全设备和传统安全设备进行整合，形成安全资源池，实现安全设备服务化和管理集中化；通过 API 方式与云平台进行联动；

资料来源：公司官网，渤海证券

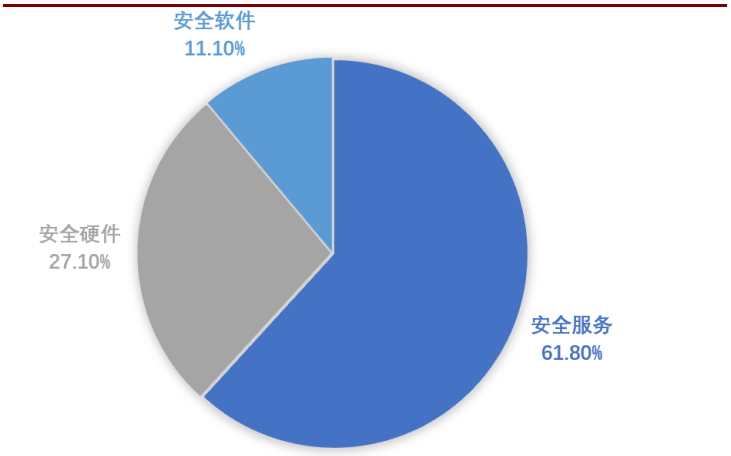
随着等保 2.0 将云安全平台作为重点等保对象，我国云安全的合规需求会推动云安全市场进一步加速发展。在合规需求与云端数据泄露压力双重推动下，云安全

市场发展空间巨大。

3.2 安全服务领域市场需求广，增量空间大

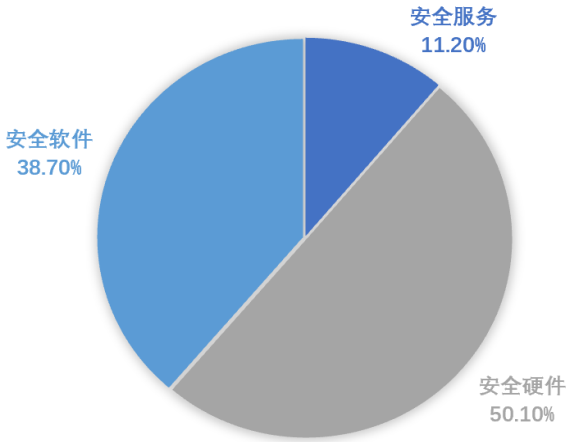
当前阶段，我国安全服务市场在整个网络安全行业中所占比重远低于国外水平。根据赛迪顾问的数据，全球网络安全市场中，2017 年安全服务市场占比超过 60%，且安全服务市场增速也快于安全产品市场。我国网络安全市场则呈现相反的格局，安全产品市场占比较大，安全硬件和安全软件合计占比达到 88.8%，安全服务市场只占据了 11.2%。

图 26：全球网络安全市场结构



资料来源：赛迪顾问，启明星辰公告，渤海证券

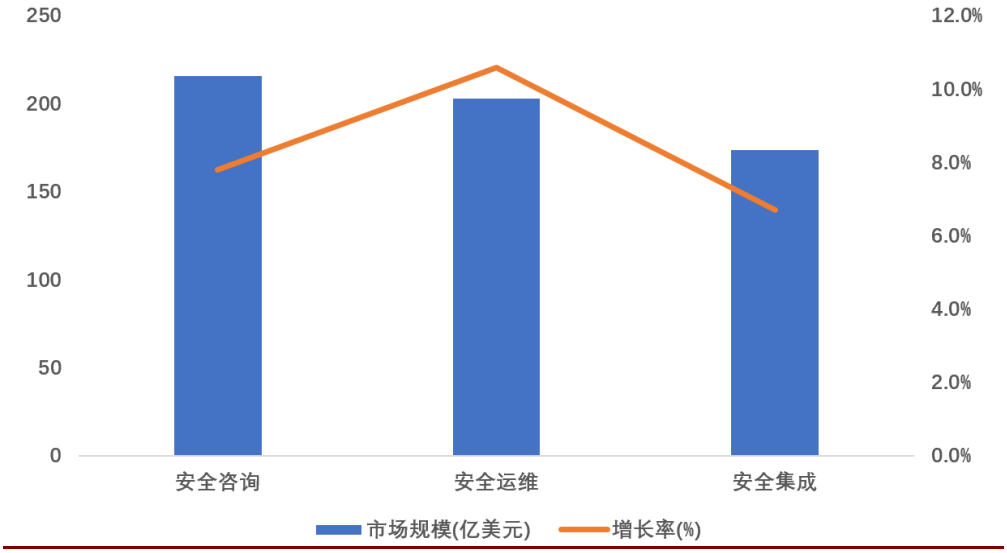
图 27：我国网络安全市场结构



资料来源：赛迪顾问，启明星辰公告，渤海证券

据 Gartner 统计，2017 年全球安全服务市场规模约为 592 亿美元，比 2016 年增长 8.3%。其中安全咨询服务市场规模最高，达到 216 亿美元，在安全服务市场中占比为 21.8%；安全运维服务市场规模 203 亿美元，同比增速为 10.6%，是安全服务市场增长的重要动力。当前，由于高级威胁等网络攻击事件数量迅速增长且攻击模式越发复杂，政府组织和企业对于安全专家与产品的协同配合要求不断提高，尤其是在当今安全技术人才匮乏的环境下，企业自身的安全人员很难完全满足企业的安全防护需求，因此依赖于第三方的安全运维服务在全球范围内增长十分迅速。

图 28：2017 年全球安全服务市场



资料来源：Gartner，中国信通院，渤海证券

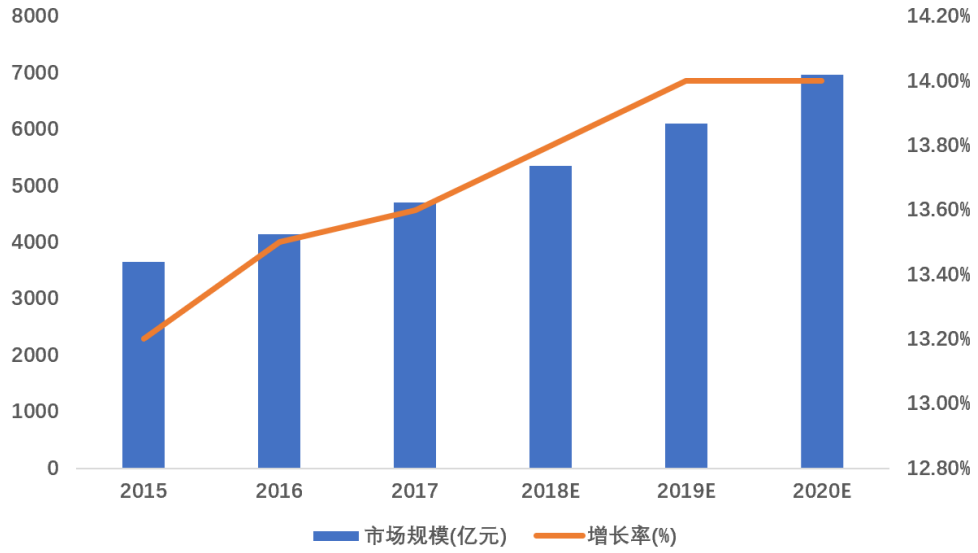
对比全球市场，我国以安全咨询、安全运维和安全集成为代表的网络安全服务市场存在较大的发展空间，市场对安全服务的需求也逐渐增强。这主要是因为随着新一代信息技术的发展和新应用场景的不断涌现，人们面临的网络环境更加复杂，信息与网络乃至应用终端的安全问题均比一般互联网的信息安全问题要多，传统的产品化、单一功能化的业务模式已经无法满足客户对信息安全的需求。在美国，已经大量出现将安全产品、安全服务一揽子外包的安全服务模式。在未来，我国网络安全市场必将向国际市场趋近，市场结构由安全产品向安全服务为主转换，以满足下游客户更多样化、个性化的安全需求。

3.3 工业互联网市场开启，工控安全前景广

根据我国工业互联网产业联盟的定义，其本质是“以机器、原材料、控制系统、信息系统、产品以及人之间的网络互联为基础，通过对工业数据的全面深度感知、实时传输交换、快速计算处理和高级建模分析，实现智能控制、运营优化和生产组织方式变革。”网络、数据和安全是工业互联网的三个重要维度。

2017 年，我国工业互联网市场规模约为 4709 亿元，比 2016 年增长 13.6%。赛迪顾问预计到 2020 年工业互联网市场规模可达到 6964 亿元，年均增长率为 13.93%。我国工业互联网正处于加速发展阶段。

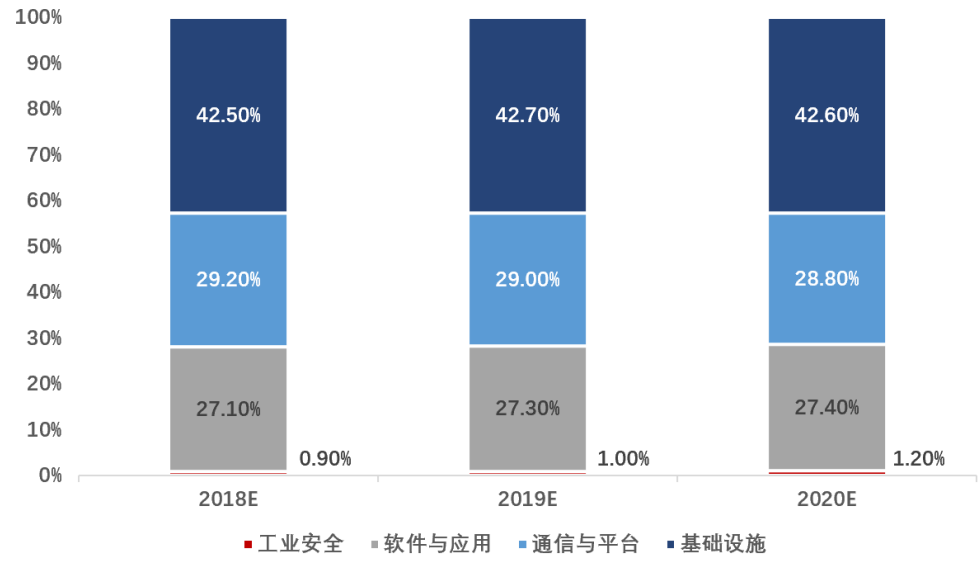
图 29：我国工业互联网市场规模及增速



资料来源：赛迪顾问，渤海证券

据赛迪顾问测算，2017 年我国工业信息安全产业在整个工业互联网市场中的占比只有 0.8%。整个工业互联网市场中占比最大的是基础设施部分，占比约为 41%；通信与平台、软件与应用两部分占比较为接近，合计占比约 58%。安全产业在工业互联网市场中的比重与其对整个产业的重要性严重不匹配。工控安全市场有望迎来快速发展的时期。

图 30：我国工业互联网市场产业结构预测

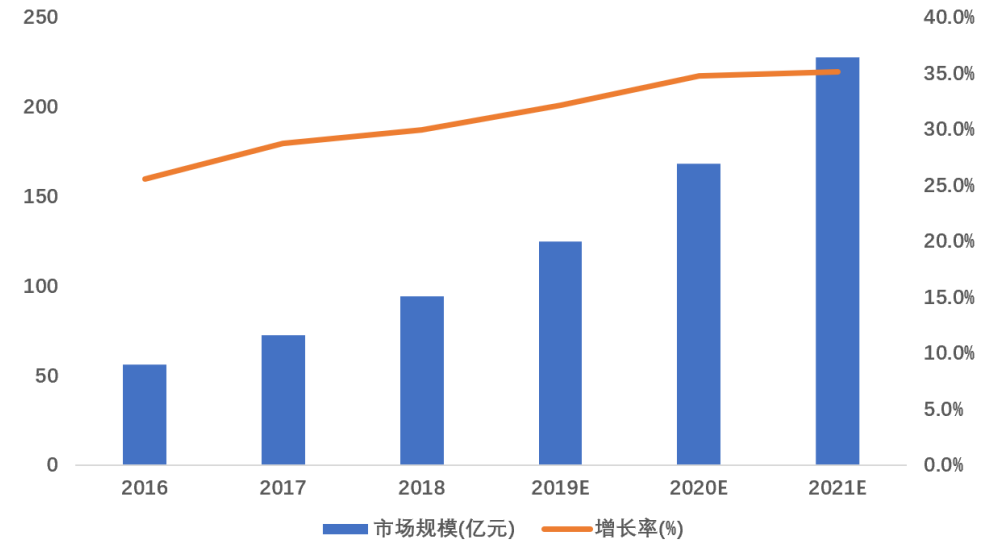


资料来源：赛迪顾问，渤海证券

2018 年，我国工业互联网安全市场规模约为 94 亿元，相比 2017 年增长 30，高于工业互联网市场增速，也高于我国网络安全市场平均增速。预计未来三年工业

互联网安全市场将保持 30%以上高速增长，到 2021 年市场规模达到 228 亿元，市场成长性较高。

图 31：我国工业互联网安全市场规模及增长率



资料来源：赛迪顾问，渤海证券

同时政府对工业互联网安全的关注不断提升，围绕《网络安全法》《中国制造 2025》，密集出台多项政策、指南以推进工业互联网安全产业的发展。

表 6：近年来我国在工业信息安全领域的重要法规政策

时间	政策	要点
2016 年 5 月	《关于深化制造业与互联网融合发展的指导意见》	促进技术融合与理念融合相统一，推动制造企业与互联网企业在发展理念、产业体系、生产模式、业务模式等方面全面融合，构建开放式生产组织体系，大力发展个性化定制、服务型制造等新模式；
2016 年 7 月	《国家信息化发展战略纲要》	从安全和发展辩证关系、信息技术战略目标、网络安全内在规律和防御威慑网络能力四个方面，对我国未来网络安全工作做出顶层设计；
2016 年 12 月	《“十三五”国家信息化规划》	强调完善网络空间治理体系、健全网络安全保障体系；
2017 年 12 月	《工业控制系统信息安全行动计划(2018-2020)》	强调重点提升工控安全态势感知、安全防护和应急处置能力，建立多级联防联动工作机制，确保信息安全与信息化建设同步规划、同步建设、同步运行；

资料来源：政府网站，渤海证券

4.行业重点上市公司

4.1 中孚信息：安全保密领域龙头，核心业务稳健增长

中孚信息成立于 2002 年，是一家专注于信息安全领域的高新技术企业，公司是国家商用密码产品定点生产和销售单位，拥有国家保密局颁发的国家涉密集成甲级资质证书，在信息安全保密领域市场优势明显。公司主营产品及服务包括信息安全保密产品、商用密码产品、信息安全服务三大类。

其中安全保密产品是公司的支柱性业务，其中最核心同时也最具有优势的产品则是涉密计算机及移动存储介质保密管理系统(简称“三合一”)，其是首批通过国家保密主管部门测评的同类产品，有助于涉密单位保密综合防护体系的建设。

表 7：中孚信息主要安全保密产品

产品名称	代表图片	产品说明
涉密计算机及移动存储介质保密管理系统(三合一)		“三合一”是一款专用的保密防护系统，具有检测阻断涉密计算机违规联接互联网、移动存储介质管理、外部数据单向导入三项功能。其由用户端软件、涉密专用优盘、多功能导入装置、保密管理中心和违规外联监控互联网报警平台五大部分构成，可有效解决涉密计算机及移动存储介质保密管理薄弱的问题。
互联网接入口保密检测器及监测平台		部署在单位互联网接入口，监测并及时阻止网络攻击行为和违规在互联网上传输敏感信息行为，具备木马监测、敏感信息检测、可疑行为检测、图文内容检测等功能。其包含的监测平台主要管理前端检测器，收集处理检测器上报数据，通过大数据分析技术，有效防止敏感信息泄漏事件发生。
存储介质信息消除工具		针对存储重要敏感信息的计算机硬盘、U 盘、移动硬盘等存储介质，应用完善的数据消除算法，对所有要消除的数据进行索引，对磁盘物理扇区进行反复擦些，使被擦除的信息无法恢复。
网络物理隔离卡		在原有计算机上增加一块硬盘，通过物理隔离卡控制硬盘及切换网线，在内外网的环境中使一个硬盘仅对应一个网络有效，其网络物理连线是完全分离的且不存在公用存储信息，从而实现一台计算机在两个网络之间安全隔离。

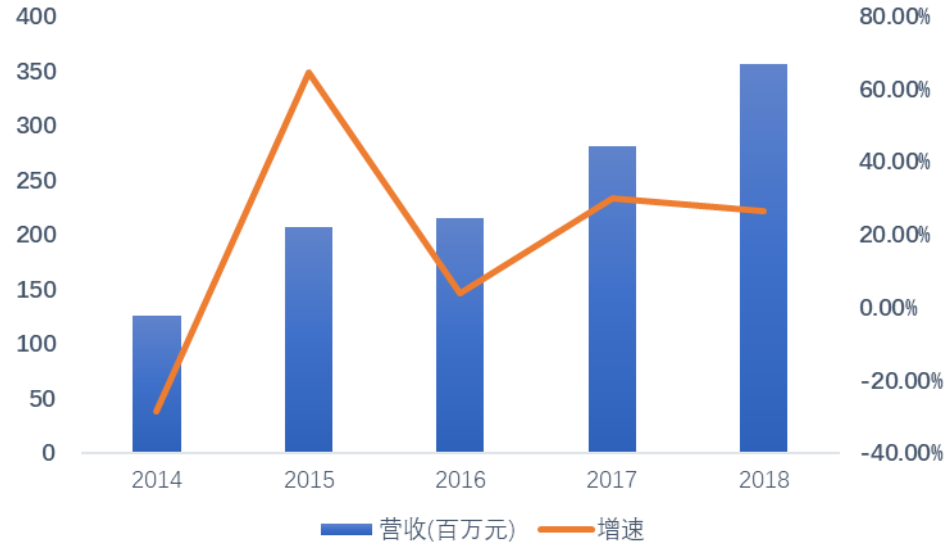
资料来源：中孚信息官网，招股说明书，渤海证券

2018 年，公司信息安全服务业务成长较快，实现营收 7000 余万元，同比增长超

过 200%。信息安全服务主要涉及为涉密信息系统集成，包括涉密系统工程的规划、设计、开发、实施、服务等工作。未来，随着企业及组织对一体化安全服务需求的增加，该板块有望成为企业快速发展的推动器。

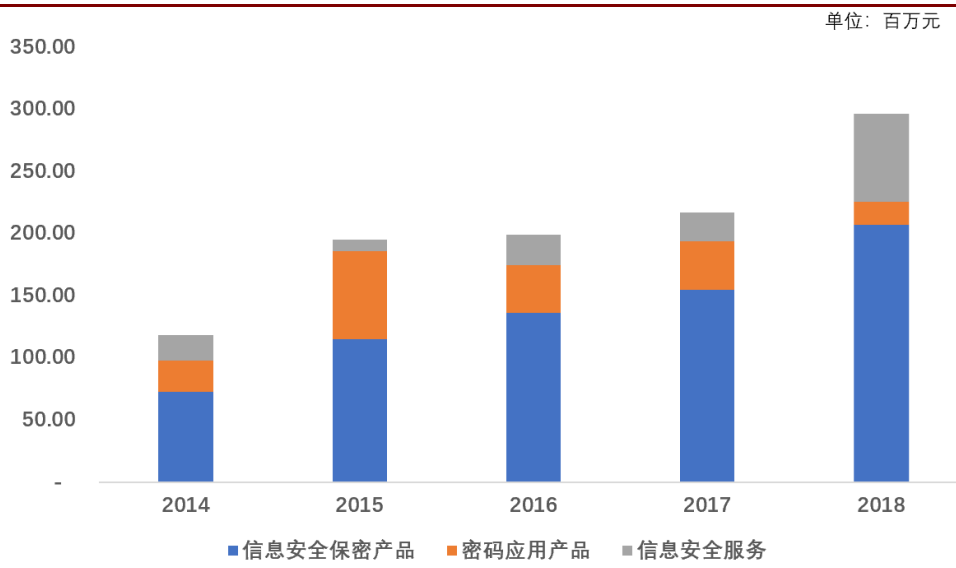
信息安全保密产品在增速和收入占比上成长稳健，该类业务 2018 年实现营收 2.07 亿元，同比增长 33.8%；2014-2018 年，安全保密产品营业收入年复合增速约为 30%。

图 32：2014-2018 年中孚信息营收及增速



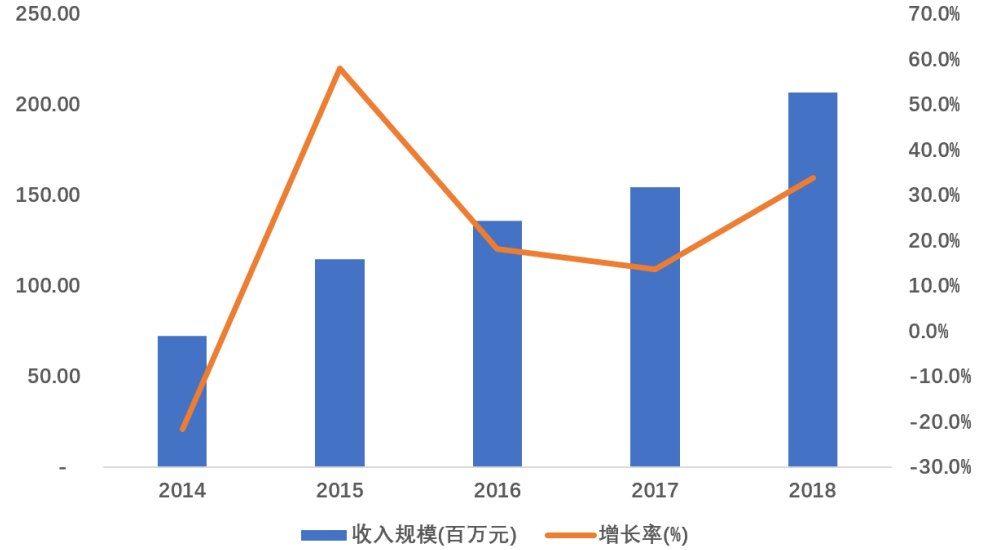
资料来源：Wind，渤海证券

图 33：2014-2018 年中孚信息主营业务构成



资料来源：Wind，渤海证券

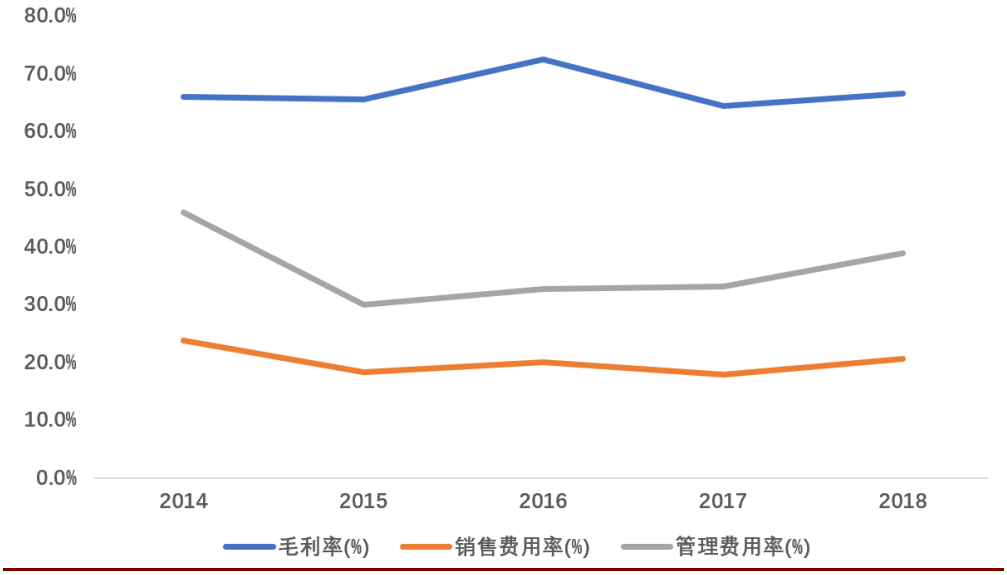
图 34：2014-2018 年中孚信息安全保密产品营收及增长率



资料来源：Wind，渤海证券

2014 年以来，公司毛利率基本稳定在 66%上下，表明核心产品销售情况稳健。费用率方面，由于公司在安全保密领域的先发优势，形成了覆盖全国的营销及服务网络，与大量党政机关和央企客户建立了良好的合作关系，因此销售费用率总体呈下降态势。管理费用因研发费用占比大、投入高，且新增股权激励的影响而上升明显，但研发投入和股权激励对公司的长期发展有较大推动作用。

图 35：2014-2018 年中孚信息毛利率与费用率



资料来源：Wind，渤海证券

伴随着各种新兴信息技术的逐渐发展成熟，公司开始逐步将安全保密产品与人工智能和大数据分析等技术相结合，推动安全保密技术从单一产品防护向防护监管一体化转变，从传统的边界防御向面向应用和数据的动态防护转变。同时，公司面向国产操作系统的安全保密产品受益于国家自主可控战略的积极推进，将会迎

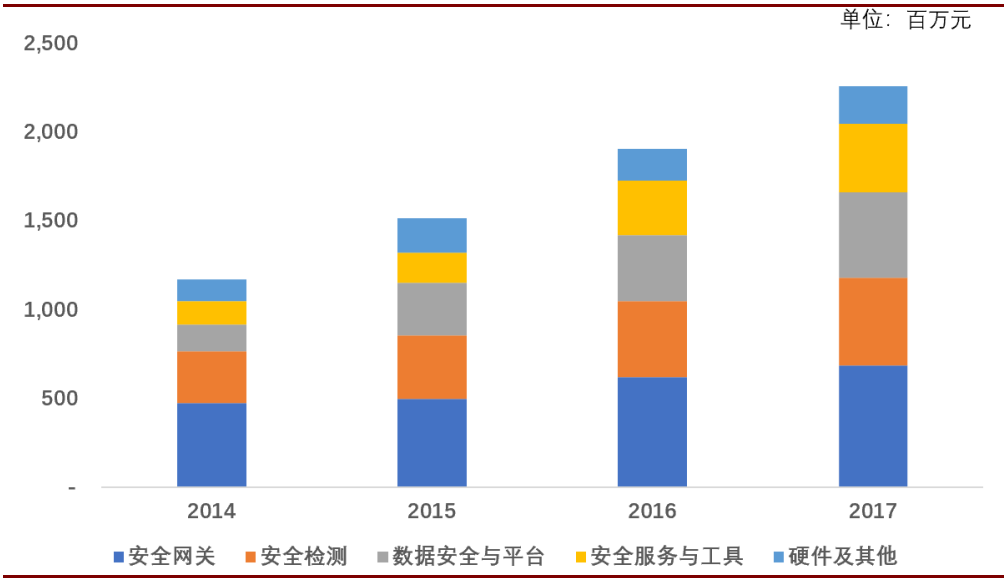
来更加广阔的发展空间，为公司未来业绩快速发展提供有力保障。

4.2 启明星辰：综合安全领先企业，新业务成长可期

启明星辰是国内成立较早、极具实力的、拥有完全自主知识产权的综合性网络安全企业。公司在网络安全软硬件产品、可信安全管理平台、安全服务与解决方案等领域均有深厚的技术积累和经验。

公司主营业务包括安全网关、安全检测、数据安全与平台、安全服务与工具、硬件及其他，其中安全网关是公司的传统核心业务，约占营业收入的 30%，占比最高。数据安全和安全服务类业务增长较快，成为推动公司发展的重要驱动力。

图 36：2014-2017 年启明星辰主营业务构成



资料来源：公司年报，渤海证券

公司是传统安全产品市场的龙头，产品线覆盖多个细分领域。公司于 2012 年收购网御星云后进入快速发展阶段，在安全硬件产品领域迅速成长为市场领导者，其产品线覆盖安全网关、安全检测、应用安全、数据安全等多个细分领域，且在国内安全网关市场、安全检测(IDS/IPS)市场，以及网闸产品市场均处于领导地位。据全球著名咨询公司 Frost&Sullivan 发布的网闸产品调研分析报告显示，截至 2016 年底，全国网闸产品的市场规模为 2.58 亿元，启明星辰子公司网御星云以 32.1%的市场份额占据头名，领先第二名近 20 个百分点，网御星云已连续 5 年市场排名第一。根据赛迪顾问的报告，2017 年公司在 IDP/IDS、UTM、SOC、数据安全产品领域市场份额排名第一。

表 8：启明星辰在安全产品领域主要产品

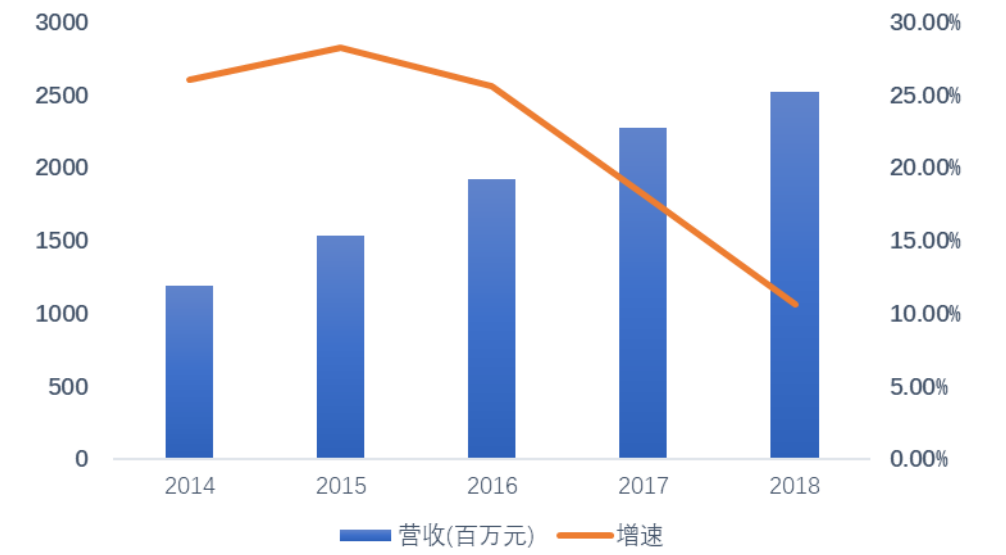
产品名称	代表图片	产品说明
天清汉马 USG 一体化安全网关(UTM)		采用业界最先进的基于多核硬件架构和一体化的软件设计，集防火墙、VPN、入侵防御系统、防病毒、上网行为管理、内网安全、反垃圾邮件、抗 DoS 攻击等多种安全技术于一身为网络边界提供全面实时的安全防护。从 2007-2016 年连续十年位居中国 UTM 市场占有率第一。
泰合安全管理平台(TSOC)		以大数据分析架构为支撑，以业务安全为导向，构建起以数据为核心的安全管理体系，强调更加主动、智能地对企业和组织的网络安全进行管理和运营。实现对海量安全信息进行全面的收集、整理、分析、审计，并借助智能化的分析手段提取出关键的安全事件。系统提供了强大的一体化安全管控功能界面，为不同层级的用户提供了多视角、多层次的管理视图。
天阗入侵检测与管理系统(IDS)		针对病毒、蠕虫、木马、DDoS、SQL 注入、缓冲区溢出等攻击行为和网络资源滥用行为等威胁具有高精度的检测能力。同时强调对威胁的可管理性，可实现只能报警分析与过滤。
天玥数据库安全审计系统		针对数据库操作行为进行细粒度审计和防护，通过对数据库管理员、业务员的数据库访问行为进行解析、记录、控制、分析，实现事前预防、始终监控、实时响应、事后追溯，是中国区数据库审计与防护第一品牌。

资料来源：启明星辰官网，渤海证券

启明星辰凭借在网络安全领域的多年经营，积累了良好的客户资源，渠道优势明显。公司在全国各省市自治区设立了三十多家分支机构，基本形成了对全国市场的覆盖。同时其下游客户分布多个重要行业，包括政府、军队、电信、金融、能源、交通、烟草、教育和传媒等多个国家重点支柱性产业的领军企业。

近年来公司营业收入增长稳健，从 2013 年的 9.48 亿元快速增长到 2018 年的 25.20 亿元，年复合增长率达到 22%。公司核心业务毛利率稳定在 75%左右，因费用控制良好，公司归母净利润从 2013 年的 1.22 亿元增长到了 2018 年的 5.69 亿元，年复合增长率达到了 36%，公司盈利能力持续提升。

图 37：2014-2018 年启明星辰营收及增速



资料来源：Wind，渤海证券

公司在保持传统安全产品领域优势地位的同时，积极布局新兴安全领域。在网络安全行业新技术不断出现，集中度逐步提升的市场变革时期，启明星辰借助完善的产品组合和强大的技术积累在安全运营、工控安全和云安全等新兴安全领域积极布局，为公司下一步的战略升级奠定了基础。

1）安全运营。公司于 2017 年 12 月在成都建开启国内首个智慧城市安全运营中心，标志着公司推进独立区域安全运营服务战略的正式落地。区域安全运营中心强调“第三方独立安全运营”，核心思想是将政府和企业的信息安全业务进行集中托管，在其自建的安全运营中心所在地独立地为各个用户提供安全运维服务，做到业务本地化。其对公司安全技术创新和整合的能力提出了全新的要求。得益于国内安全服务市场的巨大增量空间和国家大力推进信息化与智慧城市战略，公司的区域安全运营中心业务将有望迎来快速的增长。

2）工控安全。工业互联网浪潮带来了工业互联网安全产业的庞大市场，公司在工控安全领域进行了全方位的布局。从基础的工业防火墙、工控 IDS、工业网闸，到工业 SOC、网络流秩序分析等，启明星辰在工控安全领域的产品与服务不断完善。

3）云安全。启明星辰还积极切入云安全服务领域，针对私有云和混合云推出多种云安全产品和服务。由于云计算的飞速发展和等保 2.0 针对云安全方面提出多项合规要求，成为未来企业公司将持续加大在云安全领域的研发投入，开发全新的云安全资源池，提供适用于云计算环境信息系统的一体化安全解决方案。

4.3 美亚柏科：业务成长稳健，国资入股再迎发展新时期

公司是国内电子数据取证领域的龙头企业，网络空间安全及大数据信息化专家。公司自 1999 年成立以来即专注于电子数据取证领域，如今其主营业务已发展到“四大产品”+“四大服务”。“四大产品”即为电子数据取证产品、大数据信息化产品、网络空间安全产品和专项执法设备。“四大服务”是存证云+、网络空间安全服务、数据服务、培训及技术支持增值服务，四大服务依托四大产品而存在。

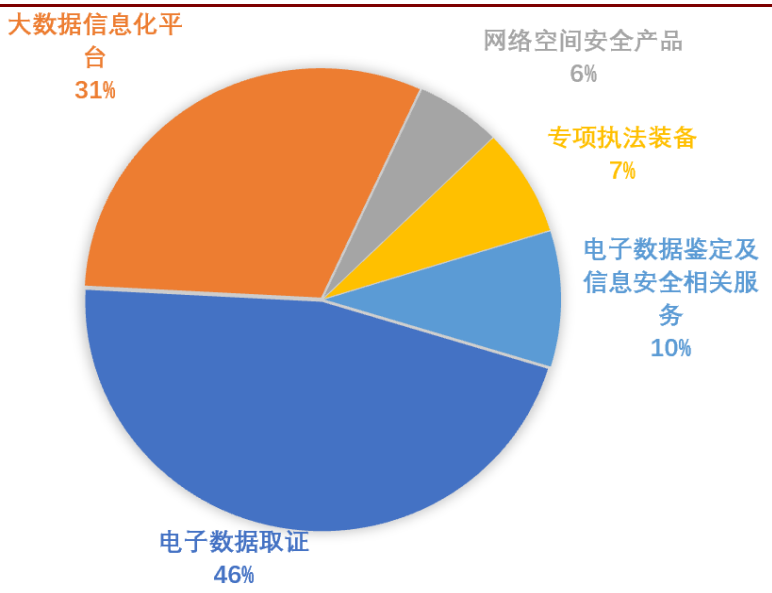
表 9：美亚柏科主要安全产品

产品名称	代表图片	产品说明
电子数据取证产品		支持对财务、计算机、手机、银行卡等电子数据进行采集、并具有对财务、计算机、手机的分析功能。数据可浏览、排序和搜索，并支持通过有效手段进行内外网隔离后上传。产品的高性能和易用性可大大提高执法效率。
网擎舆情监测系统		是一个集舆情信息的全面聚合、快速发现、智能识别、深度分析为一体的综合应用平台，利用大数据及其相关技术实现互联网舆情相关工作的简单化、智能化。版本全新升级后，在数据采集效率方面提升 30%，在数据处理方面增加众多聚类、智能学习、垃圾过滤处理等设计。
城市公共安全管理平台		在统一汇聚全市各单位具有共享价值的公共安全数据基础上，依托大数据等技术，为全市公共安全管理提供统筹研判、预防预警、应急处置、协同调度等功能服务，并与各单位的专业信息系统互为补充，构建一体化的公共安全防控体系，实现信息互通、资源共享、精细管理、数字决策，突出解决关口前移、预防预警的问题。
执法存证记录仪		集录音、录像、拍照、定位以及网络传输的执法记录终端，结合存证云全程同步存证的软硬结合服务，针对公安、交警、等执法人员使用，是公安民警应急指挥、交警、消防、海关、城管、边防等各警种的移动监控，执法过程全程同步存证，有效防止证据篡改。

资料来源：美亚柏科官网，渤海证券

电子数据取证业务是公司的核心业务，也是传统优势业务，公司在该领域处于龙头地位，市场竞争优势明显。2018 年公司电子数据取证业务实现营收 7.37 亿元，占公司总营收的 46.07%。电子数据取证是指对遭受入侵、破坏等攻击的计算机系统进行扫描和分析，对恶意犯罪行为实施证据获取、保存和分析和出示的过程。智研咨询在 2017 年发布的电子数据取证行业报告中提到，2016 年我国电子数据取证市场规模约 12 亿元，并预测到 2023 年，其市场规模将达到 35.62 亿元，年均增长率为 16.82%。

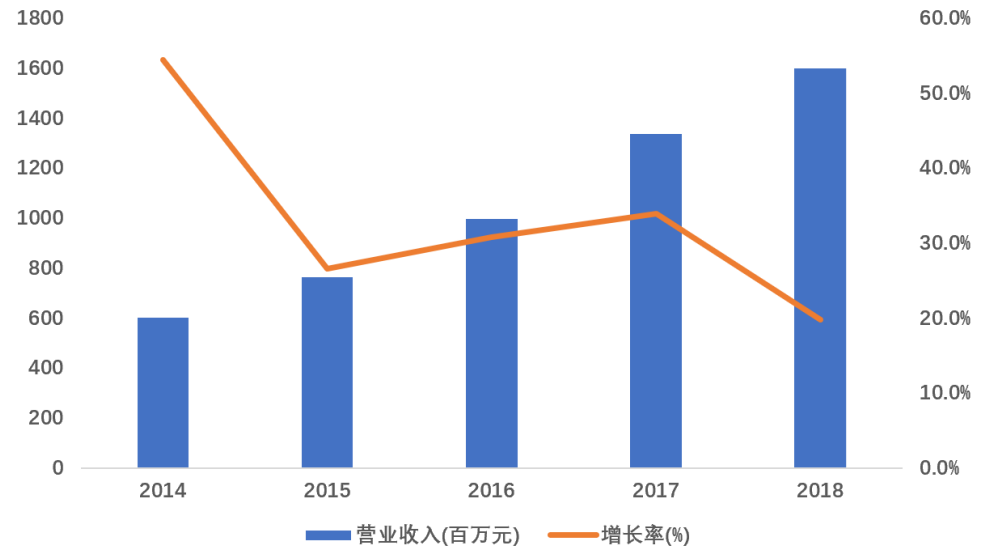
图 38：2018 年美亚柏科主营业务结构



资料来源：Wind，渤海证券

近年来公司营收增长速度较快，从 2014 年的 6 亿元快速增长到 2018 年的 16 亿元，年复合增长率为 27.64%。显示了公司较好的成长性。

图 39：2014-2018 年美亚柏科营收及增速

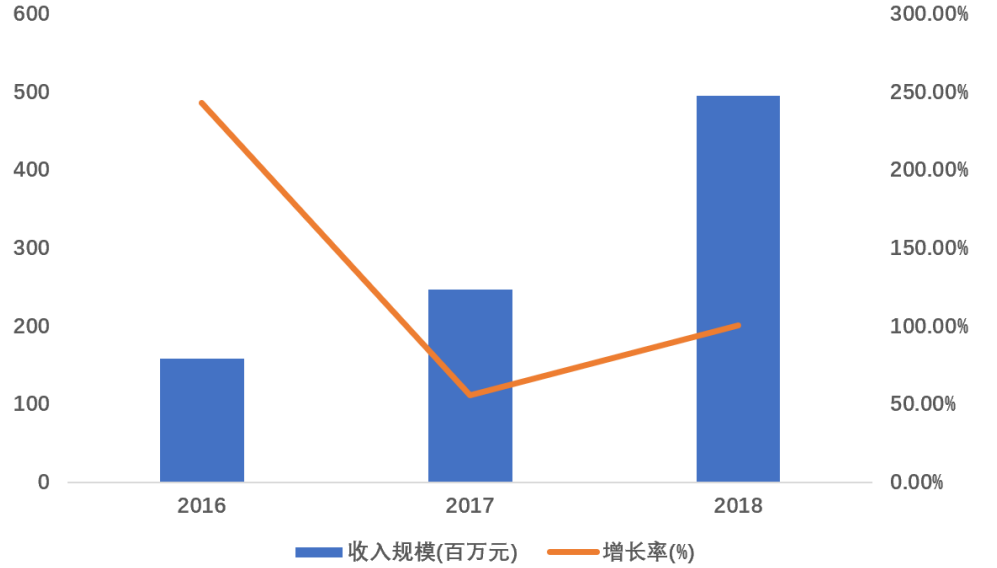


资料来源：Wind，渤海证券

公司近年来开始横向拓展大数据信息化业务，结合其在电子数据取证上的技术经验，为司法机关及行政部门建设大数据信息化平台。公司的大数据信息化业务包括司法大数据平台，城市公共安全平台，海关、税务、市场监管大数据平台等，借助大数据业务，公司的下游客户对象也从政府拓展至征信、食品安全等大众领域。大数据信息化业务的拓展，让公司能更好的实现从前端产品销售到全流程信息服务的运营模式的转变，安全+大数据服务的结合将为公司带来新的发展空间。

公司大数据业务收入规模从 2016 年的 1.59 亿元增长到 2018 年的 4.96 亿元，年均增速高达 77%，成为推动公司增长的重要驱动力。

图 40：美亚柏科大数据信息化业务收入规模及增长率



资料来源：Wind，渤海证券

2019 年 3 月 29 日，公司与国投智能签署了《股份转让协议》，如果转让完成，国投智能成为公司控股股东。国投智能是国家开发投资集团在互联网和大数据产业的战略投资平台，进驻美亚柏科意味着国家对大数据及网络安全领域的高度重视。利用国投智能的平台与资源优势，公司未来在信息安全及大数据领域的成长潜力将得到进一步释放，有利于公司提高行业地位和综合竞争实力。

5.风险提示

网络安全政策落地进展不及预期，技术进步不及预期，行业竞争加剧等。

投资评级说明

项目名称	投资评级	评级说明
公司评级标准	买入	未来 6 个月内相对沪深 300 指数涨幅超过 20%
	增持	未来 6 个月内相对沪深 300 指数涨幅介于 10%~20%之间
	中性	未来 6 个月内相对沪深 300 指数涨幅介于-10%~10%之间
	减持	未来 6 个月内相对沪深 300 指数跌幅超过 10%
行业评级标准	看好	未来 12 个月内相对于沪深 300 指数涨幅超过 10%
	中性	未来 12 个月内相对于沪深 300 指数涨幅介于-10%-10%之间
	看淡	未来 12 个月内相对于沪深 300 指数跌幅超过 10%

免责声明：本报告中的信息均来源于已公开的资料，我公司对这些信息的准确性和完整性不作任何保证，不保证该信息未经任何更新，也不保证本公司做出的任何建议不会发生任何变更。在任何情况下，报告中的信息或所表达的意见并不构成所述证券买卖的出价或询价。在任何情况下，我公司不就本报告中的任何内容对任何投资做出任何形式的担保，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失书面或口头承诺均为无效。我公司及其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或争取提供投资银行或财务顾问服务。我公司的关联机构或个人可能在本报告公开发表之前已经使用或了解其中的信息。本报告的版权归渤海证券股份有限公司所有，未获得渤海证券股份有限公司事先书面授权，任何人不得对本报告进行任何形式的发布、复制。如引用、刊发，需注明出处为“渤海证券股份有限公司”，也不得对本报告进行有悖原意的删节和修改。

渤海证券股份有限公司研究所

所长&金融行业研究
张继袖
+86 22 2845 1845

副所长&产品研发部经理
崔健
+86 22 2845 1618

计算机行业研究小组
王洪磊（部门经理）
+86 22 2845 1975
张源
+86 22 2383 9067

汽车行业研究小组
郑连声
+86 22 2845 1904
陈兰芳
+86 22 2383 9069

食品饮料行业研究
刘瑀
+86 22 2386 1670

电力设备与新能源行业研究
张冬明
+86 22 2845 1857
刘秀峰
+86 10 6810 4658
滕飞
+86 10 6810 4686

医药行业研究小组
赵波
+86 22 2845 1632
甘英健
+86 22 2383 9063
陈晨
+86 22 2383 9062

通信行业研究小组
徐勇
+86 10 6810 4602

公用事业行业研究
刘蕾
+86 10 6810 4662

餐饮旅游行业研究
刘瑀
+86 22 2386 1670
杨旭
+86 22 2845 1879

非银金融行业研究
洪程程
+86 10 6810 4609

中小盘行业研究
徐中华
+86 10 6810 4898

机械行业研究
张冬明
+86 22 2845 1857

传媒行业研究
姚磊
+86 22 2383 9065

电子行业研究
王磊
+86 22 2845 1802

固定收益研究
冯振
+86 22 2845 1605
夏捷
+86 22 2386 1355
朱林宁
+86 22 2387 3123
李元玮
+86 22 2387 3121

金融工程研究
宋旸
+86 22 2845 1131
李莘泰
+86 22 2387 3122
张世良
+86 22 2383 9061

金融工程研究
祝涛
+86 22 2845 1653
郝倞
+86 22 2386 1600

流动性、战略研究&部门经理
周喜
+86 22 2845 1972

策略研究
宋亦威
+86 22 2386 1608
严佩佩
+86 22 2383 9070

宏观研究
宋亦威
+86 22 2386 1608
孟凡迪
+86 22 2383 9071

博士后工作站
张佳佳 资产配置
+86 22 2383 9072
张一帆 公用事业、信用评级
+86 22 2383 9073

综合管理&部门经理
齐艳莉
+86 22 2845 1625

机构销售•投资顾问
朱艳君
+86 22 2845 1995
刘璐

合规管理&部门经理
任宪功
+86 10 6810 4615

风控专员
白骐玮
+86 22 2845 1659

渤海证券研究所

天津
天津市南开区水上公园东路宁汇大厦 A 座写字楼
邮政编码：300381
电话:（022）28451888
传真:（022）28451615

北京
北京市西城区西直门外大街甲 143 号 凯旋大厦 A 座 2 层
邮政编码：100086
电话：（010）68104192
传真：（010）68104192

渤海证券研究所网址：www.ewww.com.cn