

中国网络安全产业白皮书



中国信息通信研究院
2022年1月

版权声明

本白皮书版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。



前 言

强大的网络安全产业实力是保障我国网络空间安全的根本和基石。近年来，习近平总书记多次就网络安全产业作出重要指示，强调“要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态”，为网络安全事业高质量发展指明方向，并提供根本遵循。

为护航制造强国、网络强国及数字中国建设，产业界共同努力，推动网络安全产业发展进入“快车道”。2020年我国网络安全产业规模较2019年增长10.6%，企业发展态势总体良好，技术创新高度活跃，生态建设不断完善，综合实力显著增强，为保障国家网络空间安全做出重要贡献。

在工业和信息化部网络安全管理局指导下，我院连续六次发布中国网络安全产业白皮书。本报告所研究的网络安全产业，主要聚焦在政策、资本、生态环境等外部因素影响下，网络安全供需双方主体通过市场机制作用，进行一系列研发、生产、经营、采购等活动所形成的组织业态。为了构建清晰的研究脉络，本报告首先对网络安全市场规模和结构总体情况进行概述，然后对国内外政策、技术产品体系、企业经营、资本赋能、产业生态等内外部因素的最新发展动态进行重点分析，多维度展现我国网络安全产业发展态势。希望为关注网络安全产业发展的政府机构、企事业单位以及相关组织和个人提供参考和帮助。

目 录

一、 全球网络安全产业发展动态.....	1
(一) 全球网络安全市场增速回落，结构分布稳中有变.....	1
(二) 网络安全政策举措纵深推进，优化产业发展环境.....	5
(三) 市场主体发展总体良好，新兴厂商优势凸显.....	9
(四) 资本加持重点领域，融资并购出现两极分化.....	13
二、 我国网络安全产业进展.....	18
(一) 网络安全市场发展稳中向好，区域行业差异明显.....	19
(二) 政策体系不断完善，推动产业发展迈向新阶段.....	22
(三) 技术产品体系持续演进，为产业发展注入动能.....	28
(四) 市场主体发展放缓，大型企业具备竞争优势.....	30
(五) 资本赋能效应显现，投资主体进一步丰富.....	35
(六) 生态建设持续优化，构筑高质量发展屏障.....	38
三、 我国网络安全产业发展举措建议.....	43
(一) 加速完善政策措施，筑牢网络安全坚实防线.....	44
(二) 持续强化技术创新，提升产业供给水平.....	44
(三) 不断优化素质结构，完善人才梯队建设.....	45
(四) 科学统筹要素资源，优化产业生态环境.....	45

图 目 录

图 1	2014-2021 年全球网络安全市场规模及增速	2
图 2	2020 年全球网络安全市场区域分布情况.....	3
图 3	2020 年全球网络安全服务市场及构成情况.....	4
图 4	2020 年全球网络安全产品市场及构成情况.....	5
图 5	2020 年国际主要网络安全上市企业营收情况.....	10
图 6	2020 年国际主要网络安全上市企业净利润情况.....	11
图 7	2020 年国际主要网络安全上市企业研发费用情况.....	12
图 8	2020 年国际网络安全企业价值与营收关联性.....	13
图 9	2011-2020 年网络安全初创企业融资态势	14
图 10	2020 年网络安全初创企业融资分布（按季度&按轮次）	15
图 11	2020 年全球网络安全融资领域分布情况.....	16
图 12	2011-2020 年全球网络安全并购活动态势	17
图 13	2020 年全球网络安全并购领域分布情况.....	18
图 14	2015-2021 年我国网络安全产业规模增长情况	19
图 15	2020 年网络安全市场营收区域结构.....	20
图 16	2020 年网络安全市场营收行业结构.....	20
图 17	2020 年网络安全营销网络覆盖省份数量.....	21
图 18	2020 年网络安全市场销售模式构成.....	22
图 19	我国网络安全法律法规体系归纳.....	23
图 20	我国网络安全法律法规数量变化趋势.....	24
图 21	产业未来三年将重点研发的新技术/新产品方向	29
图 22	市场现有产品和服务所覆盖的新兴领域情况.....	29
图 23	市场认为未来最有发展潜力的网络安全新技术/新理念	30
图 24	2020 年我国主要网络安全上市企业营收情况.....	31
图 25	2020 年我国主要网络安全上市企业季度营收增速情况.....	32
图 26	2020 年我国主要网络安全上市企业净利润情况.....	33
图 27	2020 年我国主要网络安全上市企业研发费用情况.....	34

图 28	2020 年我国网络安全企业价值与营收关联性.....	35
图 29	2020 年我国网络安全企业价值与利润关联性.....	35
图 30	2020 年我国网络安全初创企业融资态势.....	36
图 31	2020 年我国网络安全融资领域分布情况.....	37

表 目 录

表 1	2020 年国际网络安全企业 IPO 情况.....	12
表 2	2020 年中国网络安全领域典型并购案例.....	38

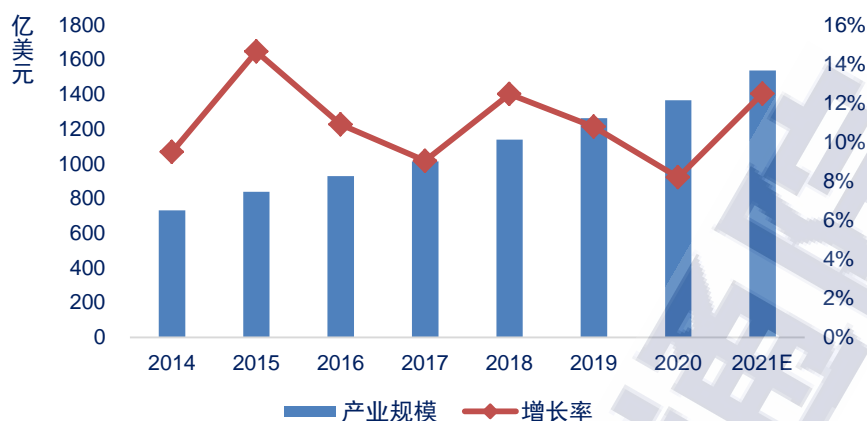
一、全球网络安全产业发展动态

2020年，受疫情影响，全球网络安全市场增速回落，市场构成发生渐进式调整，政策、企业、资本等内外部因素助推网络安全发展。具体来看，政策方面，以美国、欧盟、澳大利亚、新加坡为代表的国家地区纵深推进网络安全政策举措，为产业发展创造良好环境。市场主体方面，网络安全上市企业营收普遍增长，新兴厂商发展较快。资本方面，网络安全融资热度攀升，并购交易降温。

（一）全球网络安全市场增速回落，结构分布稳中有变

1.2020年全球市场规模增长情况好于预期

2020年全球网络安全市场规模为1366.6亿美元，同比增长8.2%，增速低于2019年同期水平，但高于2020年6月Gartner预测数据，这一超预期增长反映了全球范围内对网络安全的迫切需求。此外，得益于市场对远程办公技术和云安全的长期需求，预计2021年产业规模将达到1537.3亿美元，同比增长12.5%；未来五年（2020~2025年）全球网络安全市场规模复合年均增长率为10.8%。

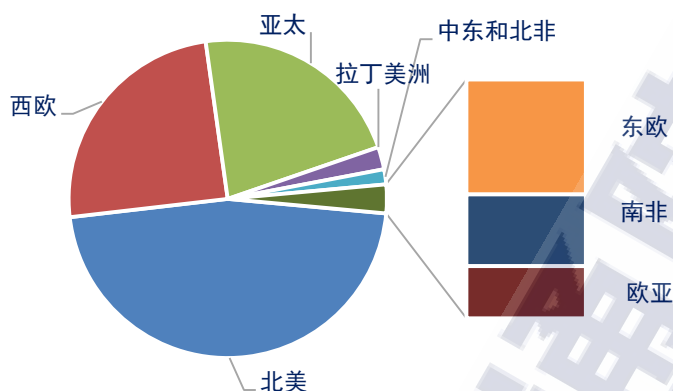


来源：Gartner

图 1 2014-2021 年全球网络安全市场规模及增速

2. 美欧亚地区三足鼎立，亚太地区更具发展活力

在地区分布方面，北美、西欧和亚太地区位列全球网络安全市场份额前三强。其中，北美占据显著优势地位，西欧和亚太则构成了另外两极。从市场份额来看，2020 年三大地区合计市场份额为 93.3%，与 2019 年同期相比，北美和西欧的市场份额略微下降，中国和新兴亚太市场的快速发展推动整个亚太地区市场份额占比提升 0.4 个百分点。从具体支出来看，北美地区 2020 年网络安全支出为 638.3 亿美元，同比增长 10.6%。西欧地区网络安全支出为 336.4 亿美元，同比增长 11.7%。亚太地区网络安全支出为 300.1 亿美元，同比增长 8.1%；其中，中国在亚太地区的增速最高。



来源: Gartner

图 2 2020 年全球网络安全市场区域分布情况

3. 网络安全市场构成正发生渐进式调整

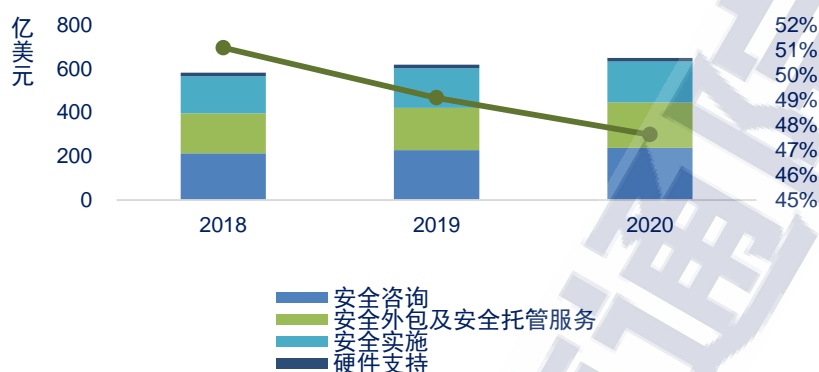
根据 Gartner 统计数据, 产品市场整体增速显著高于服务市场¹, 服务市场规模占比正在逐年降低。继 2019 年网络安全产品市场规模首次超越网络安全服务后, 该趋势在 2020 年得到进一步加深, 2020 年网络安全服务市场规模占比降至 47.6%。

2020 年全球网络安全服务市场规模为 650.7 亿美元, 同比增长 4.95%。从细分类别来看, 安全咨询类服务是 2020 年安全服务中最大的支出类别, 支出规模为 238.6 亿美元, 在安全服务中的占比为 36.7%; 安全外包及安全托管服务²为第二大支出类别, 支出规模为 207.5 亿美元, 在安全服务中的占比为 31.9%。从各类别增速来看, 安全外包及安全托管服务近年来发展势头强劲, 2020 年该类别支出

¹ 本小节中安全服务市场仅涉及安全咨询、安全外包及安全托管服务、安全实施、硬件支持四大类。

² 安全托管服务: Managed Security Services(MSS), Gartner 将 MSS 定义为通过远程安全运营中心(SOC)而非现场人员提供的 IT 安全功能的远程管理和/或监控。

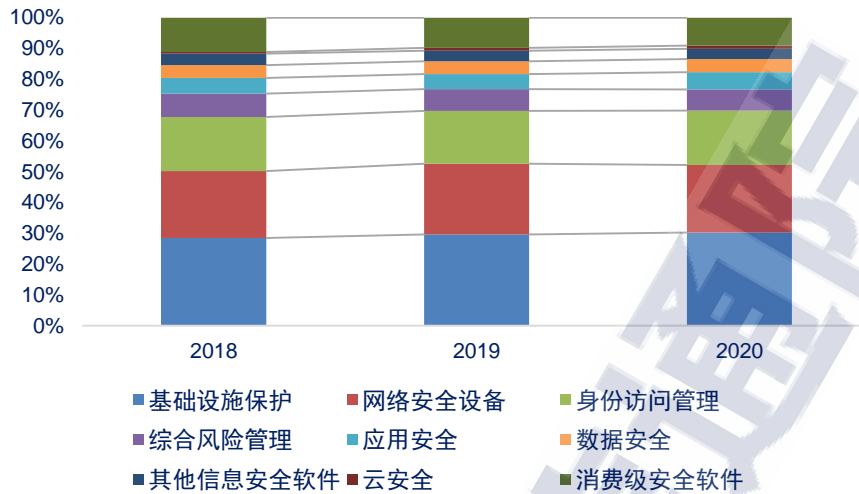
同比增长 7.3%，远高于安全服务平均增速。



来源：Gartner

图 3 2020 年全球网络安全服务市场及构成情况

2020 年全球网络安全产品市场规模达到 715.9 亿美元，较 2019 年增长 11.2%。从细分类别来看，市场份额最高的三类依次是基础设施保护、网络安全设备和身份访问管理。其中，基础设施保护类产品的市场规模为 217.0 亿美元，占比为 30.3%；网络安全设备类产品的市场规模为 156.3 亿美元，占比为 21.8%；身份访问管理类产品的市场规模为 126.9 亿美元，占比为 17.7%。从各类别增速来看，云安全、应用安全成为极具发展前景的两大细分领域，虽然目前市场规模较小，但两大领域均以超过 30% 的增速迅速壮大。



来源: Gartner

图 4 2020 年全球网络安全产品市场及构成情况

(二) 网络安全政策举措纵深推进，优化产业发展环境

1. 美国为维护领导者地位持续深化战略布局

美国为保持其在未来科技领域的领先地位，持续调整其网络安全战略布局。顶层路线方面，2021年3月，白宫发布《国家安全战略临时指导方针》，将提升网络安全作为美国政府首要任务，鼓励私营部门与各级政府合作，同时加大基础设施投入，保卫美国免受恶意网络活动侵害。2021年5月，拜登签署《改进国家网络安全行政令》，提出预防、检测、评估和处置网络安全事件是国家和经济安全的重中之重。组织机构调整方面，2021年1月美国国务院批准设立新的网络空间安全和新兴技术局（CSET），该组织负责与美国盟友和伙伴国开展合作，推动网络空间安全和新兴技术相关工作。该项调整直接体现美国保障新技术安全和加强国际合作的网络安全

战略重点。**新技术领域安全方面**，美国将人工智能、能源、量子信息科学、通信和网络技术、半导体和太空技术作为关键和新兴技术，不断强化上述领域的网络安全治理。2020年9月，白宫发布《太空网络安全指令》，提出保护太空系统免受网络威胁和网络攻击的建议和最佳实践。2021年2月，美国国家网络安全卓越中心发布《5G网络安全实践指南》草案，作为5G网络安全实践指南的第一册，旨在帮助5G网络运营商和用户减轻5G网络安全风险。**网络安全能力方面**，一方面美国持续推动网络安全架构演进。2021年2月，美国国家安全局发布《零信任安全模型指南》，敦促整个国防部及其承包商对敏感系统实施零信任。2021年9月，美国管理和预算办公室发布《联邦零信任战略》草案，指导、牵引、推动政府机构将其网络安全架构从传统架构向零信任架构转变。另一方面，美国开始通过网络安全成熟度模型认证法规来加强其网络安全能力。2020年12月，美国防部公布了首批需要通过网络安全成熟度模型认证（CMMC）的15个项目，要求国防部承包商需通过独立的第三方CMMC审核，确保其具备与业务相当的网络安全级别。**国际合作方面**，美国加强与同盟和伙伴在网络安全方面的合作，促进情报共享。2020年10月，新美国安全中心提出建立民主技术政策联盟框架，强调需要在理念相近的国家间进行广泛长期的多边合作，利用多边出口管制措施等方法维护技术竞争优势。2021年2月，美国网络安全与基础设施安全局发布新的全球国际合作战略，通过加强国际合作以增强关键基础设施的安全性和弹性。

2. 欧盟升级安全战略为数字化转型保驾护航

为全面提升在数字经济领域的竞争优势，维护自身的“数字主权”，欧盟多措并举促进其网络安全战略升级。一是提升网络安全核心战略地位。2021年3月提出的“2030年欧洲数字化转型愿景”，以及欧盟新型研究与创新项目“地平线欧洲”等战略计划均将网络安全作为其发展重点板块。2021年3月，欧盟理事会通过了欧盟数字十年网络安全战略，旨在增强欧洲抵御网络威胁的应变能力。二是推动出台新技术应用的安全保障措施。2020年11月，欧盟网络安全局ENISA发布《物联网安全准则》，提供涵盖物联网供应链，包括硬件、软件和服务在内的整个物联网生命周期安全指南。2021年4月，欧盟委员会发布人工智能规则提案和协调计划，要求确保欧盟市场AI系统的安全性。三是不断完善数据安全保障措施。2020年11月，欧盟委员会提出《数据治理法规》，以促进欧盟内部数据共享。2021年4月，欧盟网络安全局发布报告《欧盟数字战略自主的网络安全研究方向》，报告确定了七个关键研究领域，以加强欧盟数字自治。

3. 澳大利亚频繁部署加快网络安全战略谋化

为维护国家安全，澳大利亚加快完善网络安全举措。一是强化整体网络安全战略，2020年8月，澳大利亚政府发布《2020年网络安全战略》，依据该战略，澳政府将投资16.7亿美元用于建立新的网络安全和执法能力，协助行业加强自我保护，并增强社区对保护在线安全的理解。2021年4月，澳大利亚政府发布《国际网络和关

关键技术参与战略》，用于指导澳大利亚在网络和关键技术问题上的国际参与决策，帮助其拥抱巨大创新机会并减轻或避免相关风险。

二是加速推进云安全布局，2020年7月，澳大利亚发布《云安全指南》，为政府和整个行业安全使用云服务提供支撑。

三是重视小企业网络安全，2021年2月，澳大利亚网络安全中心更新《小企业网络安全指南》，旨在帮助小型企业保护自己，免受传统的网络安全事件影响。

四是持续更新在线安全法案，2021年2月，澳大利亚更新《在线安全法案 2021》，保护网络空间中澳大利亚公民，尤其是儿童的在线安全。

4.新加坡提升网络安全水平开启新发展蓝图

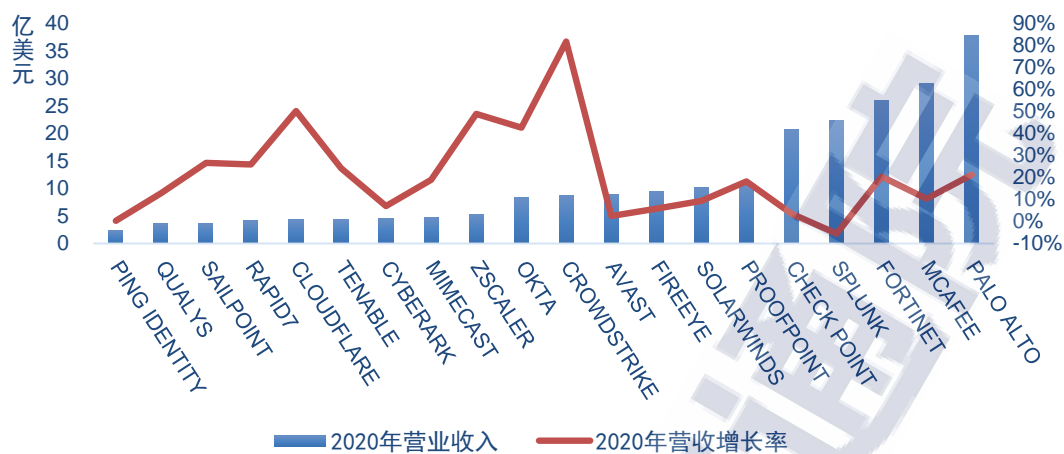
新加坡不断完善网络安全防范体系，为“智慧国家”战略愿景提供坚强助力。在安全规划方面，2020年10月，新加坡启动《新加坡更安全的网络空间总体规划（2020年）》，提出了三大战略目标及保护核心数字技术设施、实施5G网络安全计划等11项安全措施。在数据安全及个人信息保护方面，2020年11月，新加坡更新《个人数据保护法》，引入了强制性数据泄露通知制度，并对数据泄露处以更严厉的罚款。2021年3月，新加坡个人数据保护委员会更新《PDPA下的数据泄露管理和通知指南》，通过数据泄露管理计划来识别和防范数据泄露。在网络安全技术方面，2021年1月，新加坡金融管理局发布修订后的《技术风险管理指南》，为金融机构提供风险缓解策略，帮助其适应新兴技术和网络威胁领域的快速变化。在国际合作方面，2021年8月，新加坡与美国达成三项协议，

双方将扩大金融、国防领域网络安全合作，通过加强信息共享、研究和培训等，解决全球网络安全问题。

(三) 市场主体发展总体良好，新兴厂商优势凸显

1. 企业营收仍保持普遍增长，但盈利能力有待改善

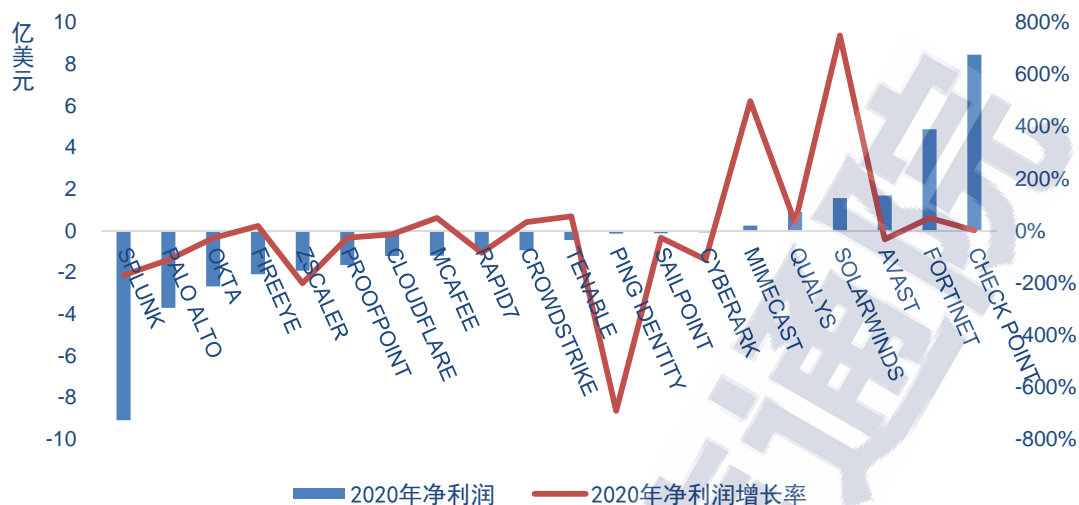
在营收方面，虽然 2020 席卷全球的新冠疫情对 IT 和互联网行业的业务发展造成一定影响，但是国际主要网络安全上市企业营收仍保持普遍增长态势。选取的专业网络安全上市企业营收数据显示，20 家国际专业网络安全上市企业 2020 年的平均营收为 11.46 亿美元，2020 年营收的平均增速为 21.23%，较 2019 年同期增速略有回落。除 Splunk 的营收出现 5.49% 的小幅下降以外，其余企业的营收均保持增长。其中，得益于新冠疫情下互联网流量激增，以及基于云计算的安全工具和安全服务的需求强劲，Cloudflare 和 CrowdStrike 的营收增速显著高于同类企业，分别达到了 50.18% 和 81.64%。数据显示，新兴的网络安全厂商处于业务创新和市场开拓的活跃期，因此安全业务营收普遍处于中高速增长期；以 Palo Alto 为代表的营收超过 20 亿美元的老牌网络安全厂商，业务发展和现金流量均处于稳健增长阶段，对应的营收增速为中低速水平。



来源：中国信息通信研究院

图 5 2020 年国际主要网络安全上市企业营收情况

在净利润方面，由于全球网络安全市场发展方兴未艾，为了获取巨大的市场机遇，该领域的企业将大量经营收入投向产品技术研发和市场营销，进而导致企业净利润持续为负。国际网络安全上市企业利润数据显示，20 家国际专业网络安全上市企业 2020 年的平均净亏损为 0.4119 亿美元，与 2019 年同期相比，亏损幅度有所增加。具体来看，除 Check Point 等少数几家企业实现盈利以外，其余企业均为亏损状态。从净利润增速来看，半数企业实现利润增长或亏损收窄，与 2019 年同期持平；其中，SolarWinds 净利润在 2020 年实现高速增长（受所得税影响较大），Mimecast 实现扭亏为盈，Ping Identity 的亏损程度进一步加剧。

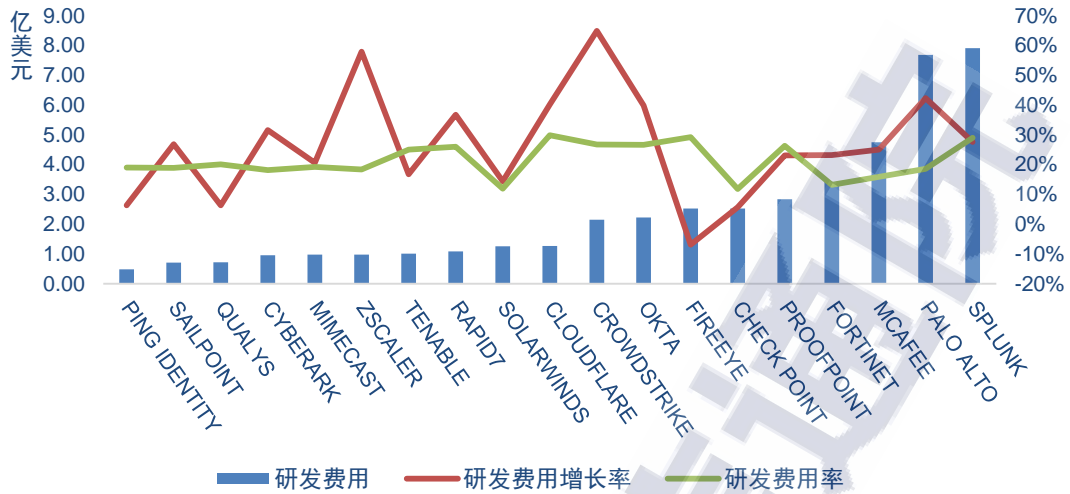


来源：中国信息通信研究院

图 6 2020 年国际主要网络安全上市企业净利润情况

研发费用方面，2020 年国际主要网络安全上市企业研发投入普涨，研发投入占营收比例保持高位。19 家主要网络安全上市企业 2020 年的平均研发费用达到 2.39 亿美元，比 2019 年高出 0.5 亿美元；Splunk 和 Palo Alto 的研发费用接近 8 亿美元，显著高于其他同类企业。研发费用增速方面，所选企业的研发费用平均增速为 26.47%，除 FireEye 的研发费用小幅下降以外，其他企业均保持较快增长，其中 Zscaler 和 CrowdStrike 的增速分别达到了 57.95% 和 64.89%，服务于企业的业务布局和核心竞争力的提升。研发费用率³方面，19 家主要网络安全上市企业的平均值为 21.16%，新兴网络安全企业的研发费用率高于老牌网络安全上市企业，这与企业的发展阶段和业务模式强相关。

³ 研发费用率=近三年研发费用之和/近三年营业收入之和。



来源：中国信息通信研究院

图 7 2020 年国际主要网络安全上市企业研发费用情况

2. 网络安全新上市企业表现强劲

据不完全统计，2020 年有 3 起网络安全 IPO，较 2019 年减少了 1 起。2020 年 IPO 的平均融资额为 4.37 亿美元。2020 年国际网络安全企业 IPO 情况如表 1 所示。

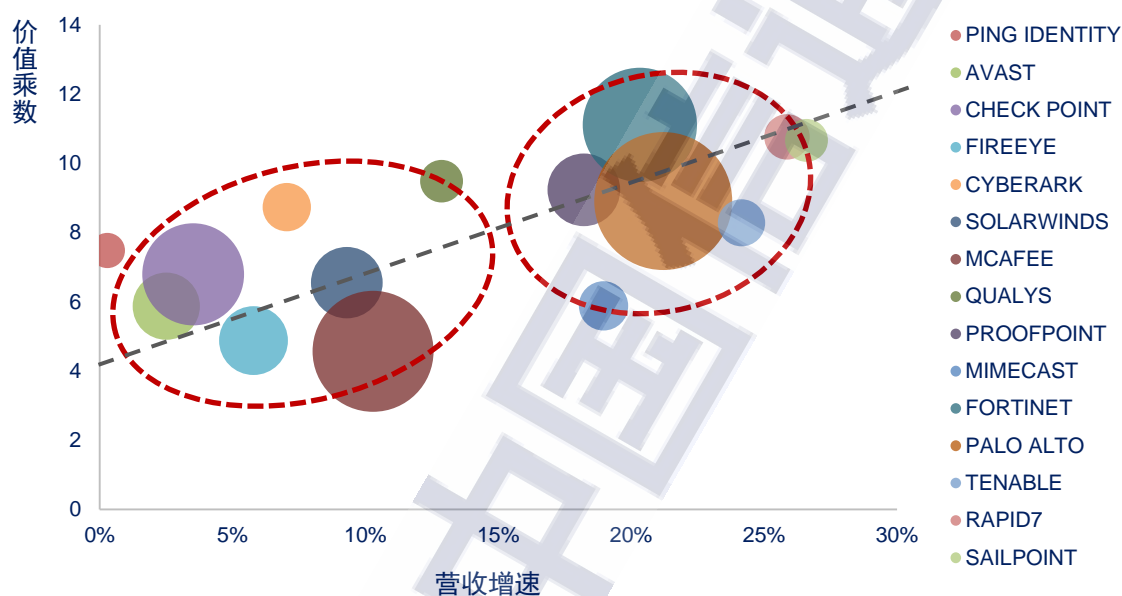
表 1 2020 年国际网络安全企业 IPO 情况

上市时间	企业名称	技术领域	上市场所
2020.09	Sumo Logic	日志管理分析	纳斯达克交易所
2020.10	McAfee	终端安全	纳斯达克交易所
2020.11	Telos	安全服务和解决方案	纳斯达克交易所

来源：中国信息通信研究院

3. 业务成长能力是企业价值增长的驱动因素

通过进一步比较分析网络安全上市企业经营业绩与资本市场企业价值的关系，发现企业价值水平和营收增速具有明显的正相关性，即营收增速较高的企业往往具有更大的价值乘数⁴；但企业价值水平和利润及其增速没有显著关系。表明国外资本市场进行网络安全投资时，更加关注公司业务本身的成长能力，而非现阶段的盈利水平。



来源：中国信息通信研究院

图 8 2020 年国际网络安全企业价值与营收关联性

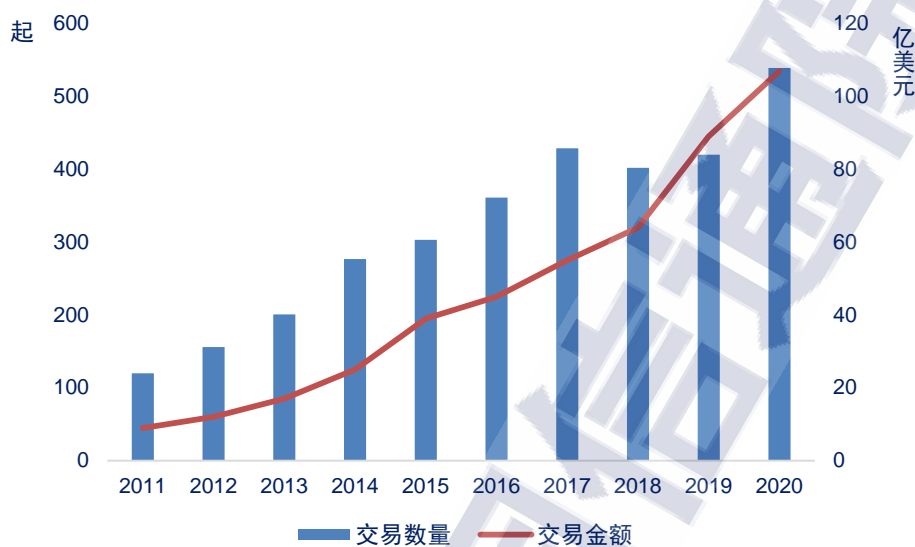
(四) 资本加持重点领域，融资并购出现两极分化

1. 融资热度攀升，交易金额首次突破百亿美元大关

2020 年，网络安全融资热度大幅攀升，成为科技主题市场融资最为活跃的领域之一。2020 年，全球网络安全融资活动为 539 起，

⁴ 企业价值乘数=Enterprise Value/Revenue，将公司价值与其收入进行比较，通常用于确定公司在潜在收购情况下的估值，可用于比较同行业公司的价值水平。

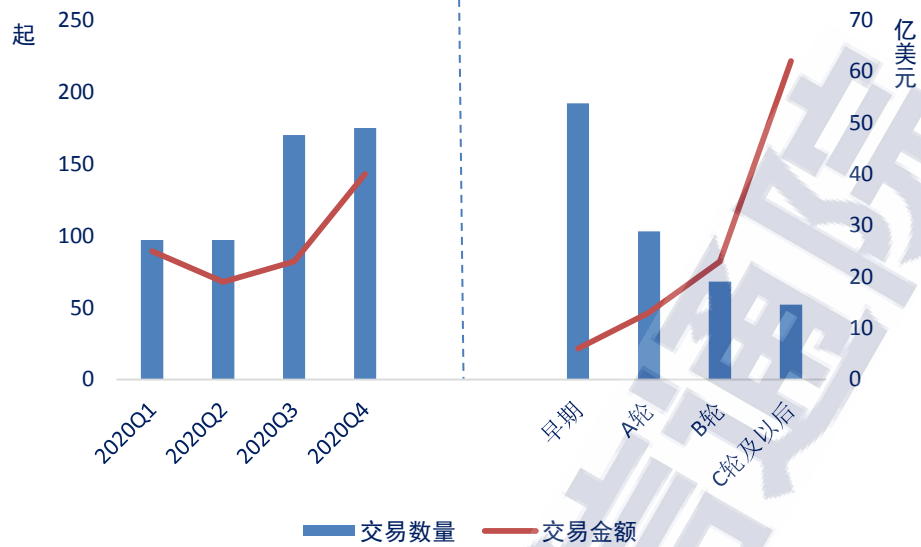
较 2019 年的 420 起大幅提高 28.33%；交易金额首次突破百亿美元大关，达到 107 亿美元，较 2019 年增长 20.22%。



来源：Momentum Cyber

图 9 2011-2020 年网络安全初创企业融资态势

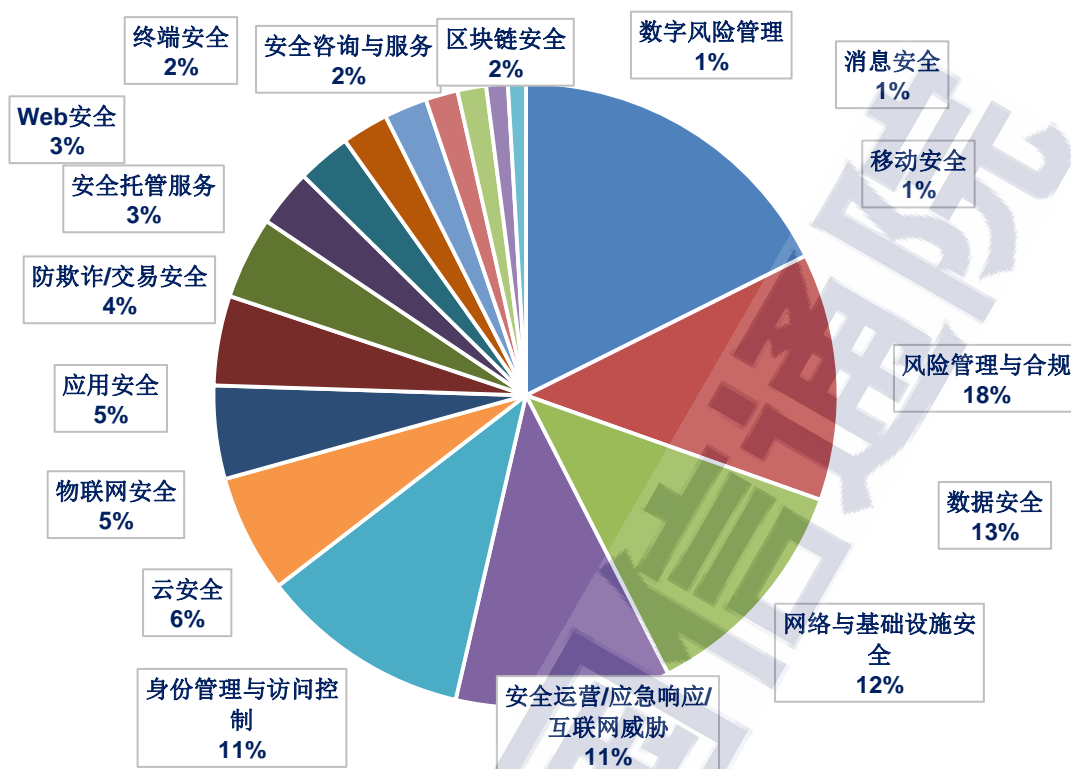
从融资时间分布看，三、四季度的融资数量较多，二者合计占全年融资总数的 64%；第四季度的融资金额最高，达到 40 亿美元，占全年融资总额的 37.4%。从融资轮次分布看，包括种子轮、天使轮、Pre-A 轮在内的早期融资案例占比 35.6%，对应的融资总额为 6 亿美元；A 轮融资案例占比 19.1%，对应的融资总额为 13 亿美元；B 轮融资案例占比 12.6%，对应的融资总额为 23 亿美元；C 轮及之后的融资案例占比 9.6%，对应的融资总额为 62 亿美元。大额融资集中在中后期阶段，其中 Rubrik、Netskope、OneTrust 单笔融资均超 3 亿美元，这表明了安全投资者对极具创新力的安全解决方案抱有极大热情。



来源: Momentum Cyber

图 10 2020 年网络安全初创企业融资分布 (按季度&按轮次)

从融资的技术领域来看，“风险管理与合规”、“数据安全”、“网络与基础设施安全”、“身份管理与访问控制”等是历年来融资较为活跃的重点领域，领域融资活动占比均超过 10%。2020 年，“风险管理与合规”领域的融资数量占比提升至 18%，“数据安全”超越“网络与基础设施安全”，排名第二，占比提升至 13%；“安全运营/应急响应/互联网威胁”相关融资数量占比由 2019 年的 9% 提升至 2020 年的 11%。

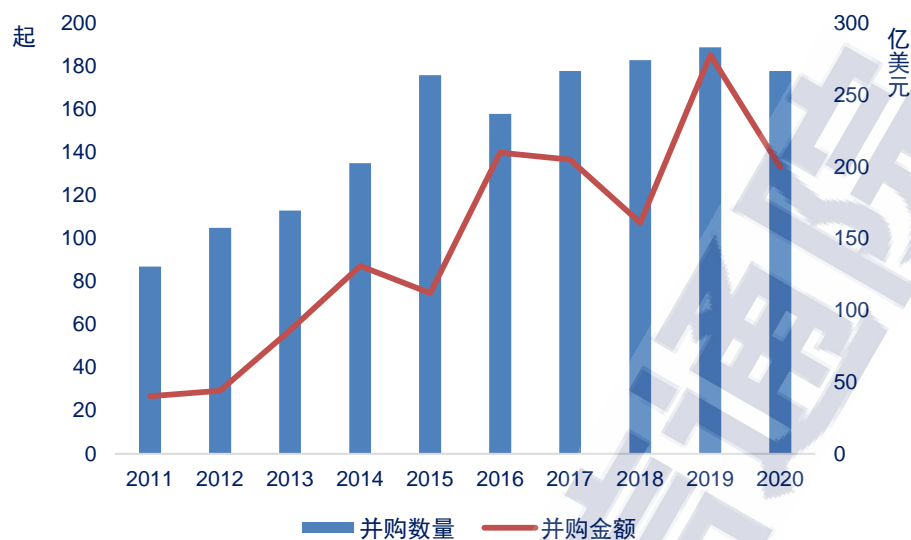


来源：Momentum Cyber

图 11 2020 年全球网络安全融资领域分布情况

2. 并购交易降温，热点领域出现新变化

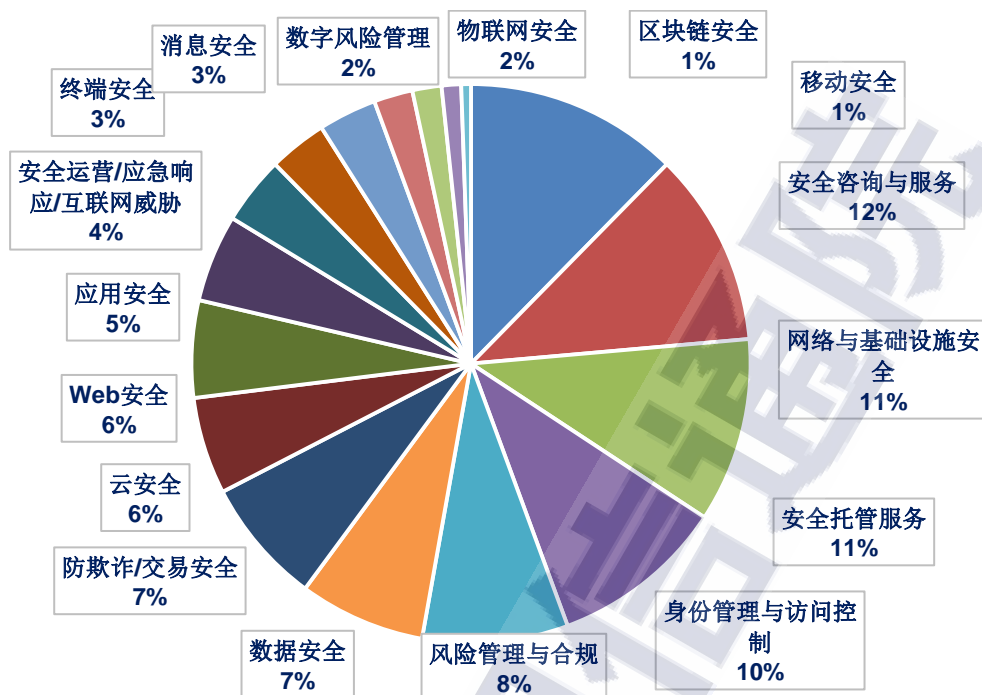
2020 年网络安全并购活动降温，并购数量和金额双双下降。据不完全统计，2020 年全球共完成了 178 起并购活动，较 2019 年下降 5.8%；并购交易金额为 200 亿美元，较 2019 年大幅下降 28.1%。



来源: Momentum Cyber

图 12 2011-2020 年全球网络安全并购活动态势

从并购的技术领域来看,安全咨询与服务、网络与基础设施安全、安全托管服务、身份管理与访问控制是 2020 年较为热门的并购领域,并购活动占比均超过 10%。与 2019 年相比,安全咨询与服务、安全托管服务的并购活动占比显著下降,与此同时,云安全、防欺诈/交易安全、数据安全、风险管理与合规领域的并购活动占比提升。2020 年,多起并购交易活动的资金规模超过了 10 亿美元,其中以 Insight Partner 为代表的私募股权公司在大规模网络安全企业收购中非常活跃,此外也有大型网络安全企业和 IT 巨头通过收购创新型企业来弥补安全技术短板。



来源：Momentum Cyber

图 13 2020 年全球网络安全并购领域分布情况

二、我国网络安全产业进展

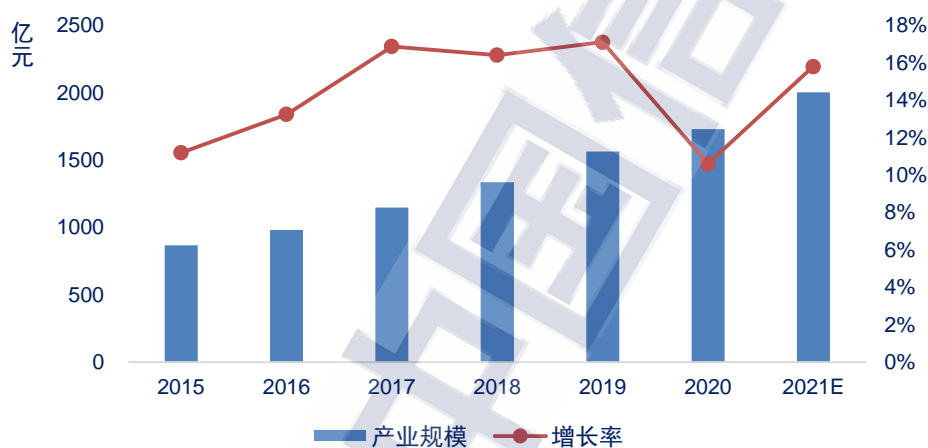
2020 年，虽然新冠疫情对我国网络安全市场造成一定冲击，市场增速出现小幅下滑，但网络安全市场总体稳中向好，政策法规、技术产品、市场主体、资本等内外部因素呈现积极变化。具体来看，政策法规方面，我国网络安全顶层设计不断完善，各地网络安全政策密集出台，推动产业发展迈向新阶段。技术产品方面，网络安全技术、理念和产品迭代升级，新场景和新技术方面布局不断优化。市场主体方面，网络安全上市企业营收增速回落，整体盈利水平优于国际同业。资本方面，网络安全融资热度不减，投资主体进一步丰富，为产业创新发展赋能。生态方面，多主体充分发挥桥梁纽带作用，产业发展要

素与资源加速聚集。

（一）网络安全市场发展稳中向好，区域行业差异明显

1.2020 年规模增速小幅下滑，预计市场将快速复苏

根据中国信息通信研究院的统计测算，2020 年我国网络安全产业规模达到 1729.3 亿元⁵，较 2019 年增长 10.6%，预计 2021 年市场将快速复苏，产业规模约为 2002.5 亿元，增速约为 15.8%。



来源：中国信息通信研究院

图 14 2015-2021 年我国网络安全产业规模增长情况

2.我国网络安全市场呈现明显的区域行业差异⁶

我国网络安全市场存在一定区域性特征，2020 年市场收入主要

⁵ 2020 年产业规模数据以国家统计局、工信部等相关单位公布的网络安全收入或增加值相关数据为基础，通过信通院网络安全产业规模测算框架进行综合测算得出。若相关基础数据由于规模以上入统企业数量或企业年度审计数据变动等原因发生调整，则后续将对相关测算数据进行同步调整。

⁶ 为充分认识我国网络安全产业运行发展态势，中国信息通信研究院面向网络安全厂商、网络安全服务商/集成商、设有网络安全事业部（子公司）的其他类型厂商（以下统称“主要网安企业”），开展了 2021 年中国网络安全企业调研。基于调研数据，得出网络安全市场在业务经营、营销渠道等方面的相关结论。

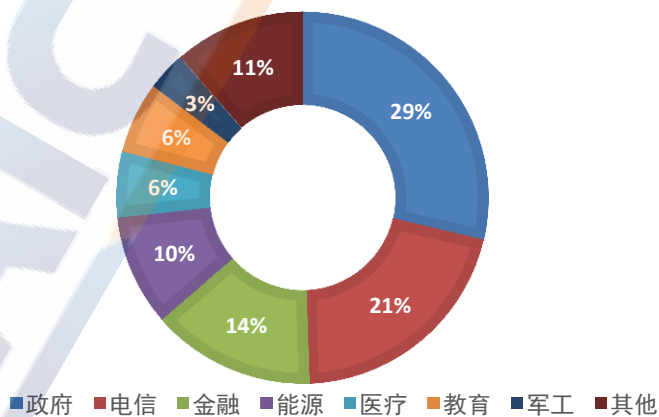
来源于华北、华南、华东三大核心区域。从本次调研数据来看，网络安全市场营收的 25.9% 来源于华北地区，25.2% 来源于华南地区，22.8% 来源于华东地区。三大核心区域合计贡献的营收占比为 73.9%。



来源：中国信息通信研究院

图 15 2020 年网络安全市场营收区域结构

网络安全产业下游客户以政府、电信和金融行业为主，三者合计占市场总营收的 64%。调研数据显示，政府和公共企事业单位仍然是当前我国网络安全产业下游的最大客户，市场营收占比为 29%；其次是电信行业，市场营收占比为 21%；排在第三位的是金融行业，市场营收占比为 14%。

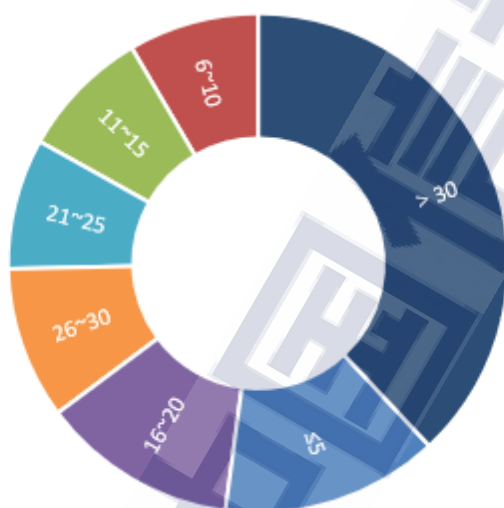


来源：中国信息通信研究院

图 16 2020 年网络安全市场营收行业结构

3.网络安全市场营销网络正在加速构建

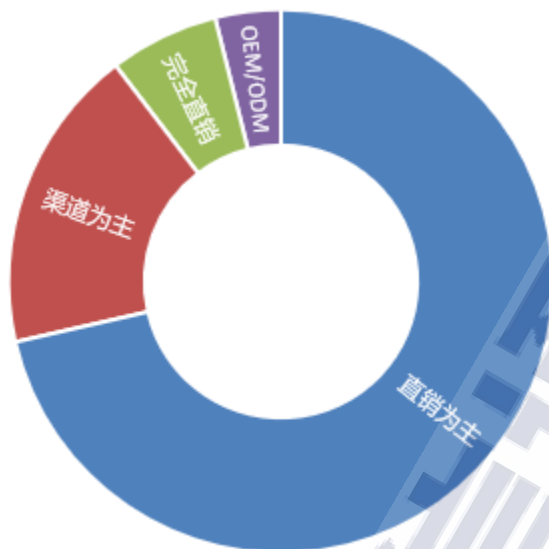
我国网络安全市场的营销网络正在加速构建。从本次调研数据来看，营销网络覆盖超过 30 个省份的厂商占比为 38%；营销网络覆盖超过 20 个省份的厂商占比为 56%。大中型网络安全企业基本建立了覆盖全国的营销网络。



来源：中国信息通信研究院

图 17 2020 年网络安全营销网络覆盖省份数量

网络安全市场多采用以直销为主的融合销售模式。从本次调研数据来看，89.6%的企业采取了直销与渠道（代理商）融合销售的方式；6.5%的企业选择采用完全直销，此类企业主要为网络安全服务商/集成商和设有网络安全事业部的其他类型厂商。在融合销售模式下，直销为主的企业占比 79.7%；渠道为主的企业占比 20.3%。



来源：中国信息通信研究院

图 18 2020 年网络安全市场销售模式构成

(二) 政策体系不断完善，推动产业发展迈向新阶段

1. 我国网络安全法律法规发展脉络逐步清晰

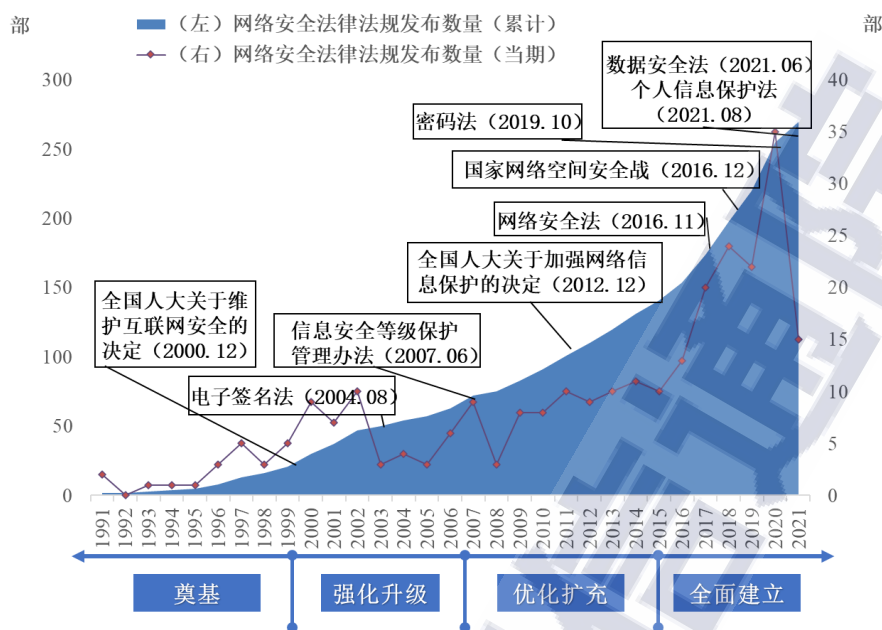
据不完全统计，截至目前，我国已出台关于网络与数据安全的法律、行政法规、部门规章、规范性文件等共计两百多部，形成了覆盖网络安全等级保护、关键信息基础设施安全保护、网络关键设备和网络安全专用产品管理、国家网络安全事件管理、密码管理、跨境活动网络安全管理、数据安全保护、个人信息保护等领域的网络安全法律法规体系。



来源：中国信息通信研究院

图 19 我国网络安全法律法规体系归纳

为了更加清晰地展现我国网络安全政策法规发展脉络，探究网络安全监管形势，综合考虑法律法规数量、效力及代表性，可以大致将我国网络安全法律法规发展情况分为四个阶段。



来源：中国信息通信研究院

图 20 我国网络安全法律法规数量变化趋势

第一阶段是网络安全法律监管**奠基阶段**（1990年-1999年），该阶段的法律法规构成了我国网络安全法律监管的雏形，但总体呈现出碎片化、分散化的特点。第二阶段是网络安全顶层制度**强化升级阶段**（2000年-2007年），该阶段我国对网络安全的重视程度提高，一些全局性的政策法规逐步出台，但大多停留在原则指导层面，尚未形成完善的体系。第三阶段是网络安全法律监管**优化扩充阶段**（2008年-2015年），该阶段有若干信息安全等级保护指导文件陆续出台，国家标准也相继落地实施，电信、金融、电力等行业出台了相关的部门规章及工作文件，推动了等级保护制度的建设，“等保1.0”体系形成。第四阶段是网络安全法律监管体系**全面建立阶段**（2016年-至今），《网络安全法》开启了我国网络安全监管和数据治理的新纪元，自此，我国逐步进入多层次、广覆盖的网络安全法

律监管体系构建阶段。

2.我国近期加大网络安全政策指导力度

在“十四五”的开局之年，网络安全成为国家安全体系能力建设的重要方向。近一年制度建设中，我国不断强化法律法规和标准规范的引导作用，积极培育促进新技术新应用落地，夯实关键信息基础设施安全保障，增强自主创新能力，建设各方面齐抓共管、共治共建的网络安全新生态。

（1）网络安全持续成为立法焦点，政策红利不断释放

近年来，我国充分发挥立法的引领和推动作用，逐步完善网络安全顶层设计。一是在推进网络安全法制建设方面取得重大进展。2021年6月，我国数据安全领域的基础性法律《数据安全法》正式发布，并于2021年9月1日起施行，数据分类分级保护、风险评估、安全审查等相关工作机制也将逐步出台。2021年8月，《关键信息基础设施安全保护条例》《个人信息保护法》相继审议通过，推动开启我国关键信息基础设施保护、个人信息立法保护的新格局，为产业发展指明方向。随着相关制度逐步完善，以数据要素赋能的“双循环”新发展格局将全面展开，产业或将迎来更为广阔的数字化发展红利。此外，《数据安全条例》《商用密码管理条例》已列入《国务院2021年度立法工作计划》行政法规制修订名单。二是将网络安全作为未来中国发展建设工作的重点之一。2021年3月，我国发布《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，共提及“网络安全”14次，涉及数字经济、数字生态、国家安

全、能源资源安全等多个领域，提出了网络安全新发展的重点思路和重点工作，为网络安全产业健康发展提出了政策保障和创新思路。

（2）新兴领域安全创新备受关注，护航能力逐渐完善

在习近平总书记关于“大力培育人工智能、物联网、下一代通信网络等新技术新应用”，“坚持安全可控和开放创新并重”的重要讲话精神指引下，工信部等部门积极采取措施，促进网络安全与新兴技术融合创新，为产业发展带来新机遇。2020年5月，工信部印发《关于深入推进移动物联网全面发展的通知》，提出加强移动物联网安全防护和数据保护，夯实移动物联网基础安全。2020年10月，国家发布《“工业互联网+安全生产”行动计划（2021-2023年）》，要求不断完善工控安全监测网络等网络安全措施，构建“工业互联网+安全生产”支撑体系。2021年3月，工信部等三部门联合印发《国家车联网产业标准体系建设指南（智能交通相关）》的通知，指导智能交通领域标准制修订，其中包括证书密钥管理、网络安全防护等两类网络安全标准。2021年6月，工信部及中央网信办印发《关于加快推动区块链技术应用和产业发展的指导意见》，提出加强区块链基础设施和服务安全防护能力建设，开展重点领域区块链技术的安全风险评估。国家政策、标准的大力推进，将充分发挥引领和规范作用，指导产业发展方向。

（3）网络安全执法力度逐步强化，需求有望快速释放

为引导企业落实网络安全主体责任，督促企业依法依规经营，国家不断加大网络安全执法力度，推进网络综合治理体系建设。2020年7月，工信部发布《关于开展纵深推进APP侵害用户权益专项整

治行动的通知》，督促相关企业强化 APP 个人信息保护，净化 APP 应用空间。仅 2021 年上半年，已连续发布五期关于侵害用户权益行为的 APP 通报，涉及 748 款软件。2020 年 8 月，六部门联合发布《教育部等六部门关于联合开展未成年人网络环境专项治理行动的通知》，通过联合开展网络环境专项治理行动，整治影响未成年人健康成长的不当网络社交行为、低俗有害信息和沉迷网络游戏等问题，为未成年人成长营造健康的网络环境。2021 年 5 月，国家网信办部署开展 2021 年“清朗”系列专项行动，组织开展治理网上历史虚无主义等八项专项行动，“重拳”整治网络违法违规问题。2021 年 7 月，国家网信办连续发布公告，对“滴滴出行”“运满满”“货车帮”“BOSS 直聘”等 APP 实施网络安全审查，审查期间将停止新用户注册，同时要求“滴滴出行”下架整改。网络空间安全整治措施的系统性推进，将大幅提升企业网络安全合规意识，激增网络安全合规体系建设需求，对于产业发展具有积极的政策导向作用。

（4）各地网络安全政策持续推进，区域产业逐步建立

各地积极推动网络安全产业高质量发展，提升网络安全产业技术水平和竞争力。一是积极出台政策措施推动产业高质量发展。2021 年 1 月，山东省印发《关于促进山东省网络安全产业发展的指导意见》，提出到 2025 年，全省网络安全产业规模突破 300 亿元。2021 年 6 月，北京发布《关于加快推进国家网络安全产业园区（通州园）产业发展若干措施（试行）》，助力将园区打造成引领国家网络安全产业发展的战略高地。二是将网络安全纳入“十四五”规划建议文件。2021 年 11 月起，各地陆续发布“关于制定国民经济和社会发展第十四个五年规

划和二〇三五年远景目标的建议”，重点包括加强网络安全保障体系和能力建设、强化关键信息基础设施安全保障能力、保障数据安全和个人信息安全、完善网络综合治理体系。同时，北京、重庆、湖北等六省市提及发挥产业集聚作用，推动网络安全产业园区建设。在各项因地制宜的政策驱动下，我们期待产业充分发挥自身优势，顺势发展，迎来爆发性增长。

(三) 技术产品体系持续演进，为产业发展注入动能⁷

1. 网络安全技术产品布局不断优化

网络安全技术创新是驱动产业发展的强大动能。各创新主体纷纷聚焦数字产业化和产业数字化发展需求，不断强化网络安全技术产品能力水平。从调研结果来看，**产业主体未来三年的重点技术和产品布局存在一定共性因素**。一是依据主体自身优势，深耕传统安全产品领域不断推动网络安全技术产品能力升级。二是面向不同应用场景，积极开展针对新兴场景的安全能力适配，提高网络安全产品专业化水平。三是主动把握技术风向标，深度探索人工智能、大数据、区块链等新兴技术在网络安全领域的应用。四是积极拥抱云模式，提升安全技术产品云化能力，构建集约化安全服务平台。五是面向差异化、多元化网络安全创新发展路径，针对零信任、可信计算等前沿技术理念开展技术攻关，推动相关产品部署落地。

⁷ 为充分认识我国网络安全产业运行发展态势，中国信息通信研究院面向网络安全厂商、网络安全服务商/集成商、设有网络安全事业部（子公司）的其他类型厂商（以下统称“主要网安企业”），开展了2021年中国网络安全企业调研。基于调研数据，得出网络安全技术产品发展方面的相关结论。



来源：中国信息通信研究院

图 21 产业未来三年将重点研发的新技术/新产品方向

2.新应用新场景带来产业发展新机遇

随着我国新型基础设施建设的全面铺开，新技术新场景驱动的网络安全需求与日俱增。监管机构已洞察到这一趋势，并进行了前瞻性的引导和部署。从本次调研数据来看，网络安全产业对新兴领域具有极大热情，积极研发相关产品和服务。其中，大数据、云计算、物联网和工业互联网是市场主体布局较多的领域。

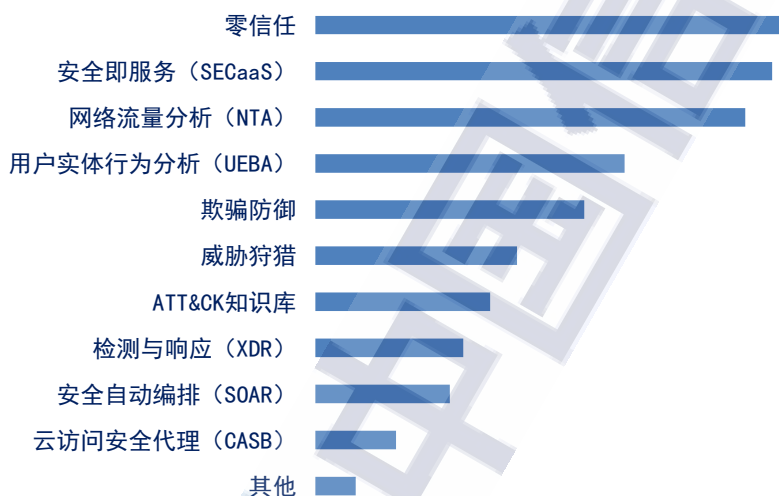


来源：中国信息通信研究院

图 22 市场现有产品和服务所覆盖的新兴领域情况

3.新技术新产品引领产业发展新方向

网络安全新技术新理念的涌现，为市场带来重构和洗牌的新机遇。本次调研结合全球网络安全相关峰会论坛、权威研究机构等对网络安全技术发展的分析研判，梳理出了业界关注度较高的网络安全前沿技术/理念。从调研数据来看，动态边界、智能分析、主动防御、云化服务是目前市场较为看好的网络安全技术发展方向。



来源：中国信息通信研究院

图 23 市场认为未来最有发展潜力的网络安全新技术/新理念

(四) 市场主体发展放缓，大型企业具备竞争优势

1. 营收增速明显回落，整体盈利水平优于国际同业

在营收方面，新冠疫情等外部因素对我国主要网络安全企业经营造成一定影响，2020年虽然大部分上市企业的营收保持增长，但是平均增速水平较去年有明显回落。选取的国内网络安全上市企业

营收数据⁸显示，20家网安企业2020年的平均营收为15.26亿元，2020年营收的平均增速为13.77%，较2019年同期水平（30.14%）明显回落。20家上市企业中，北信源、任子行和飞天诚信的营收同比下降，其余企业的营收均保持增长，2020年营收增速超过30%的企业有中孚信息、安恒信息和奇安信三家。其中，中孚信息营收快速增长的主要驱动力是数据安全产品、安全监管产品收入的高速增长；安恒信息和奇安信的营收增长则得益于云安全、大数据安全、工业互联网安全等新赛道安全产品销量快速增长，以及安全服务业务规模的进一步扩大。数据显示，我国规模体量较大的综合型网络安全厂商的营收增速高于体量较小的专精型厂商，前者对新冠疫情等外部经营风险的应对能力较强。



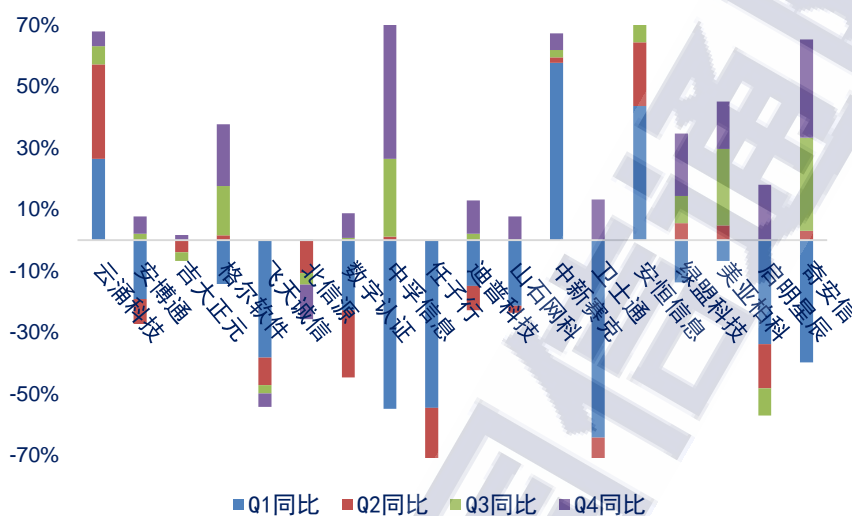
来源：中国信息通信研究院

图24 2020年我国主要网络安全上市企业营收情况

从季度营收增速来看，新冠疫情造成网络安全产业部分客户预算临时调整、商务洽谈延迟、实施交付滞后等阶段性影响，营收增速整

⁸ 为剔除非相关业务的影响，深信服和天融信的营收和净利润已根据安全业务占比进行调整。

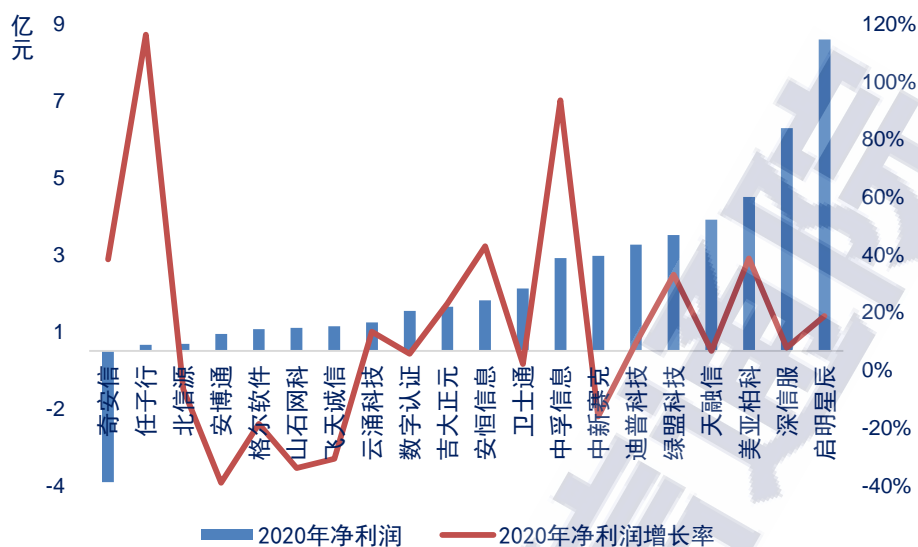
体放缓，但上述影响主要集中在上半年。2020 年一至四季度，20 家企业中当季营收同比增速为负的企业比例分别为 75%、55%、35% 和 20%，表明上市网络安全企业的经营在逐渐恢复。



来源：中国信息通信研究院

图 25 2020 年我国主要网络安全上市企业季度营收增速情况

在净利润方面，纵向比较，在市场整体大环境趋弱的形势下，我国网络安全上市企业 2020 年盈利增速高于 2019 年，体现出网络安全市场广阔的发展潜力。从企业利润数据来看，20 家网络安全上市企业 2020 年的平均净利润为 1.85 亿元，净利润平均增速为 15.28%，略高于 2019 年同期水平。与营收表现类似，我国规模体量较大的综合型网络安全厂商整体的利润增速同样高于体量较小的专精型厂商，反映出中国网安市场中规模优势与竞争优势之间的强相关性。横向比较，我国网络安全上市企业大部分已实现逐年盈利，整体盈利水平优于国际同类企业。



来源：中国信息通信研究院

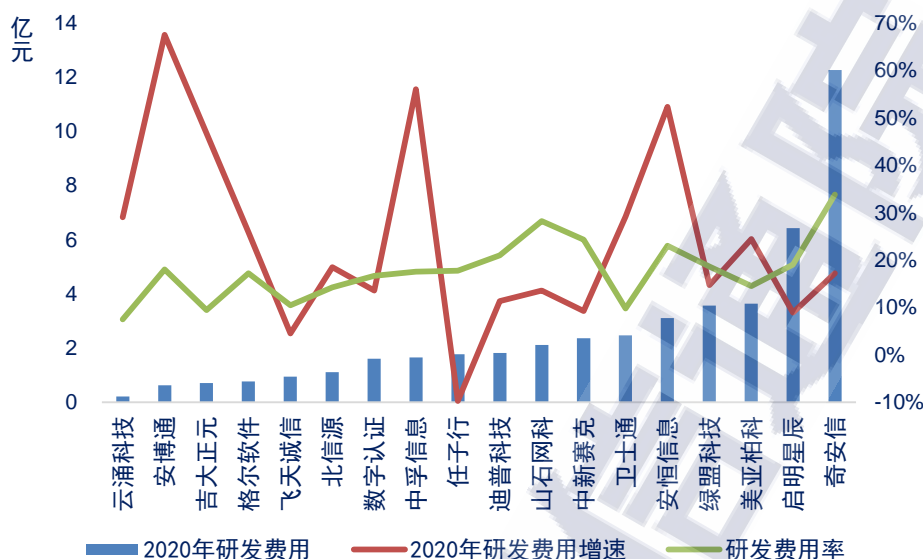
图 26 2020 年我国主要网络安全上市企业净利润情况

研发费用方面，2020 年我国主要网络安全上市企业研发投入普涨，研发费用率低于国际同业水平。18 家⁹主要网络安全上市企业 2020 年的平均研发费用达到 2.63 亿元，比 2019 年高出 0.41 亿元；奇安信的研發费用超过 12 亿元，显著高于其他同类企业。研发费用增速方面，所选企业的研发费用平均增速为 24.1%，除任子行的研发费用小幅下降以外，其他企业均保持较快增长。其中安博通、中孚信息和安恒信息的增速分别达到了 67.6%、56.1%和 52.4%，持续加大在新场景和新技术领域的研发投入。研发费用率¹⁰方面，18 家主要网络安全上市企业的平均值为 17.9%，低于国际同类企业平均水平。此外，无论是研发费用增速，还是研发费用率，企业均展现出差异化发展态势，

⁹ 深信服和天融信两家企业兼营其他业务，因此在分析网络安全研发费用时剔除二者。

¹⁰ 研发费用率=近三年研发费用之和/近三年营业收入之和。

与企业的发展阶段、业务模式和经营规模并无显著关系。



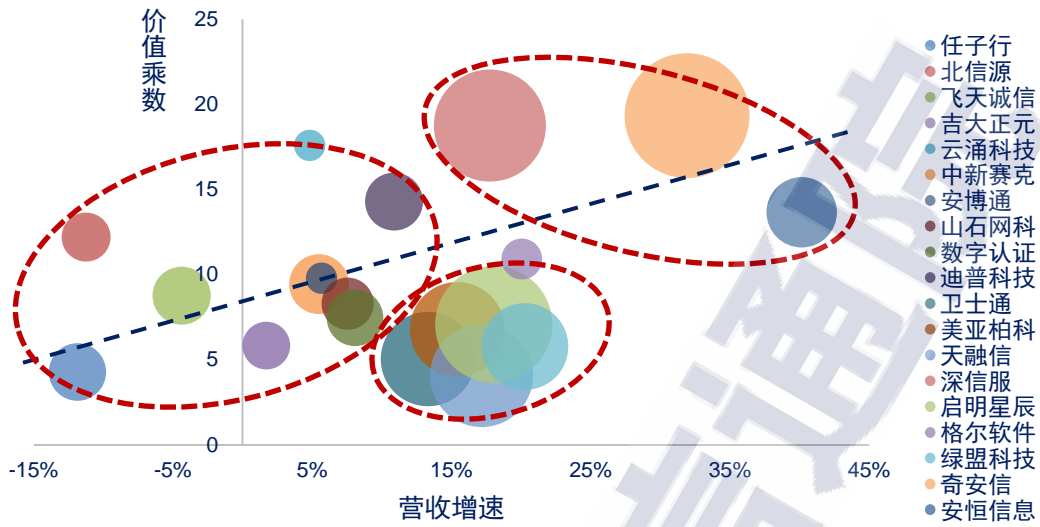
来源：中国信息通信研究院

图 27 2020 年我国主要网络安全上市企业研发费用情况

2.我国网络安全企业价值增长的驱动因素更为复杂

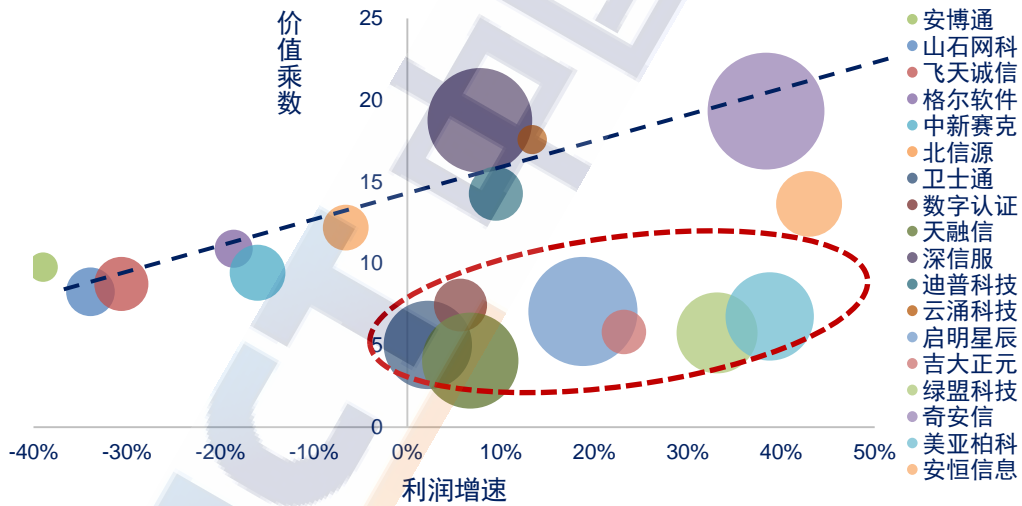
与国际网络安全资本市场相比，我国网络安全上市企业价值水平和营收增速、利润增速都有一定的相关性，但并非完全正相关，这表明国内网络安全企业价值增长的驱动因素更为复杂，需要综合考虑公司业务的增长能力、盈利能力和其他非财务因素。

与国际网络安全市场明显不同的是，一方面，企业价值更为分散，价值乘数最低值与国际市场相当，最高值接近 20 倍，比国际市场最高企业高出 9 倍；另一方面，国内资本市场对企业价值的认可出现明显的分化，一部分厂商处于高价值高增长的“双高”梯队，以此同时，一部分综合型网络安全厂商虽然业绩成长良好，但价值趋弱。



来源：中国信息通信研究院

图 28 2020 年我国网络安全企业价值与营收关联性



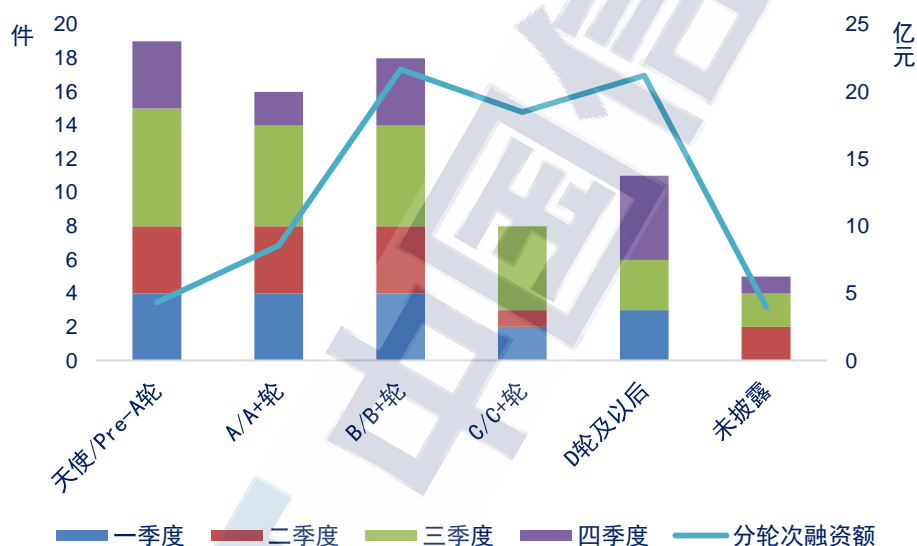
来源：中国信息通信研究院

图 29 2020 年我国网络安全企业价值与利润关联性

(五) 资本赋能效应显现，投资主体进一步丰富

1. 融资保持较高热度，数据安全成为最热门领域

2020 年我国网络安全领域融资保持较高热度。据不完全统计，2020 年我国网络安全领域的融资活动为 77 起，披露¹¹的融资总额约为 78.2 亿元。从融资案例的时间分布看，第三季度热度最高，投融资案例占全年的 38.2%。从融资轮次来看，目前我国网络安全融资活动主要集中于早中期阶段。其中，天使/Pre-A 轮融资案例数为 19 起，A/A+轮融资案例数为 16 起，B/B+轮融资案例数为 18 起，三者合计占融资案例总量的 68.8%，对应的融资金额占比约为 44.1%。



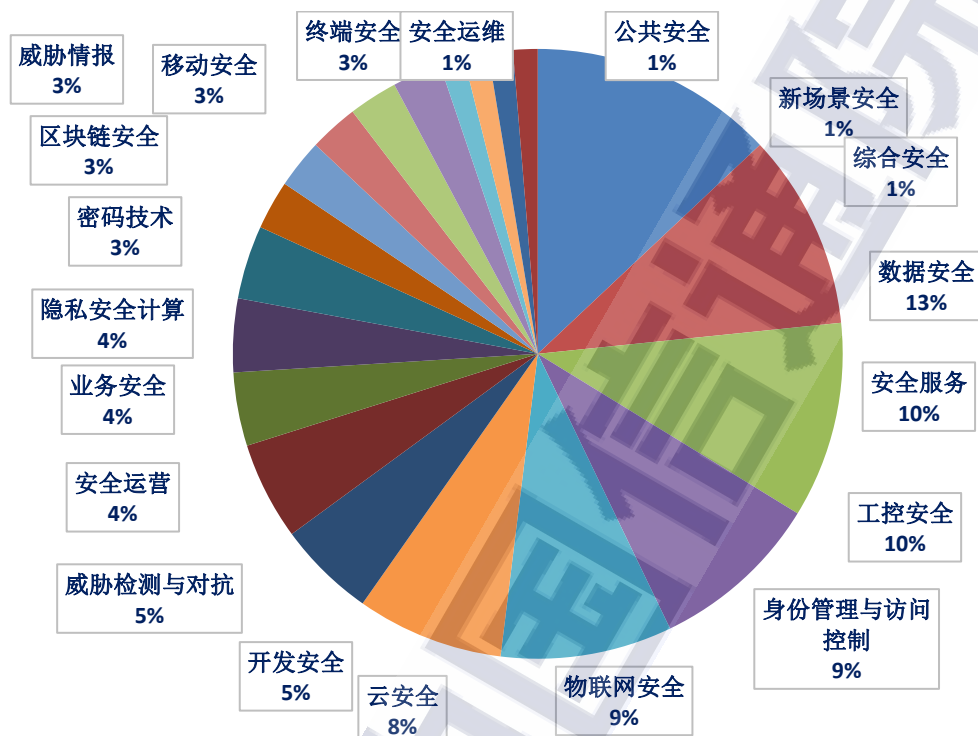
来源：中国信息通信研究院

图 30 2020 年我国网络安全初创企业融资态势

从融资的技术领域来看，数据安全、安全服务和工控安全是 2020 年较为热门的融资领域，对应的融资活动占比均超过 10%。2020 年大额融资案例数量上涨，超三成融资为亿元级别；其中，威胁检测与对抗、威胁情报、云安全、综合安全、工控安全、身份管理与访问控

¹¹ 由于多起战略投资案例未披露交易金额，可能造成该阶段交易总额被低估。

制领域均有超 3 亿元的大额融资出现，高技术能力企业的资本吸引力进一步显现。



来源：中国信息通信研究院

图 31 2020 年我国网络安全融资领域分布情况

网络安全投资参与主体进一步丰富，除了各类传统的“企业级”风险投资基金，还有更多重磅基金参与网络安全领域投资，例如：以中国国有企业结构调整基金和中国互联网投资基金为代表的“国家级”股权投资基金；以“深创投”为代表的服务于国家科技重大专项成果转化的顶级国有基金；中国电子科技集团、航天科工等央企国企旗下的投资基金；腾讯、百度等 IT 巨头设立的风投基金；服务于车联网等新兴产业发展的专业基金等。

2. 并购交易强化补充安全能力，总体规模有待提升

据不完全统计，2020 年有 4 起网络安全并购。从实施主体来看，一是互联网巨头为强化自身安全能力而进行的收购。例如，腾讯云收购玉符科技的目的在于建设 IDaaS 平台，建立起统一的身份认证体系，实现 SaaS 厂商互联互通。二是国有资本实施的收购。例如，江南信安的联合收购案例，是央企与民企共同推动网络安全产业做大做强的一次重要实践。三是网络安全企业主导的收购。例如，奇虎 360 频繁出手，实现大安全版图升级。

和国外网络安全领域并购交易的活跃态势相比，我国的并购交易数量屈指可数。目前网络安全市场企业众多，分布在各细分赛道，亟需通过并购整合和企业退出机制减少恶性竞争，降低资源内部损耗，提升规模效应和行业集中度。

表 2 2020 年中国网络安全领域典型并购案例

被收购方	收购方	收购比例	披露时间
玉符科技	腾讯投资	100%	2020.12
江南信安	共青城众智投资、中电信息、奇安基金	100%	2020.09
瀚思科技	奇虎 360	100%	2020.06
亿方云	奇虎 360	100%	2020.04

来源：中国信息通信研究院

(六) 生态建设持续优化，构筑高质量发展屏障

1. 协会联盟搭建平台助推发展

网络安全相关协会在行业自律、交流活动、人才培养等方面积极发挥桥梁纽带作用。行业自律方面，中国通信企业协会通信网络安全

专业委员会（以下简称：网络安全专委会）2020年为135家单位颁发了213个通信网络安全服务能力评定证书，促进了电信和互联网行业网络安全服务的规范开展。交流活动方面，2020年9月，中国网络空间安全协会与重庆市网信办在“2020数据安全高峰论坛”上共同发布了2020年数据安全典型实践案例，为数据安全保护提供了可供复制推广的先进经验。人才培养方面，网络安全专委会于2020年10月和2021年5月举办电信和互联网行业网络安全工作研修班，并组织网络安全人员能力认证（管理类/技术类）考试，扎实推动网络安全专业人才培养队伍建设。

为改善网络安全产业市场格局分散、细分领域碎片化、低价竞争等困境，产业联盟这一合作模式近年来逐渐兴起。一类是院企合作发起成立的网络安全联盟。2020年10月，中国信息通信研究院、三大运营商、华为、BAT、小米、奇安信等30余家业界单位联合发起成立物联生态安全联盟；2021年4月，中国信息安全研究院和奇安信集团牵头发起的“零信任”联盟，该联盟首批发起单位近50家。另一类是优势企业利用自身生态构建的联盟。2020年8月，奇安信威胁情报中心、盛邦安全、志翔科技、天际友盟等多家单位共同发起建立威胁情报生态联盟；2020年8月，华为集合国内细分领域具有竞争优势的网络安全企业、安全服务提供商组建“华为安全商业联盟2.0”；2021年3月，中国电信与国内知名高校、科研机构、网信安全软硬件系统供应商、服务提供商、系统集成商等产业合作伙伴发起成立“天翼网信安全产业联盟”。各产业联盟通过集聚高校、科研机构、上中下游供应商和服务商等众多势力，实施资源整合和协作创新，通

过在网络安全相关领域形成较大的合力和影响力，助力网络安全技术产品演进升级，从而推动产业高质量发展。

2. 国际合作开放共享积极推进

一是持续深化与东盟的网络安全合作机制。2020年11月，第23次中国—东盟领导人会议发布了《落实中国—东盟面向和平与繁荣的战略伙伴关系联合宣言的行动计划（2021-2025）》，双方就在加强网络安全产业发展、网络安全应急响应能力建设等领域开展交流合作达成一致。2021年1月，中国与印尼签署《关于发展网络安全能力建设和技术合作的谅解备忘录》，为发展网络安全能力和技术提供合作框架。二是积极参与亚太区域网络安全国际活动。2020年3月、10月，中国分别参加亚太地区计算机应急响应组织（APCERT）发起举办的2020年亚太地区网络安全应急演练，和2020年度东盟网络安全应急演练，不断增强与各国在共同保障网络安全方面的合作。2020年8月，依据2011年签订的“国家级计算机安全事件响应小组联合合作备忘录”，中日韩在线上顺利召开第八届中日韩互联网应急年会，三方就新冠疫情下网络安全事件态势以及处置措施等方面开展交流合作。三是描绘全球数字治理新图景。2020年9月，中国提出《全球数据安全倡议》，为全球数字治理规则制定贡献中国方案。2021年3月，中国同阿拉伯国家联盟共同发表《中阿数据安全合作倡议》，双方在数字治理领域达成高度共识，呼吁通过建立互信、深化合作等方式，化解各国数据安全风险。

3. 园区建设聚集资源成效显著

一是北京、长沙两地国家网络安全产业园区基本建成。2020年11月，国家网络安全产业园区（北京）通州园区正式开园，至此北京三区合力打造的国家网络安全产业园区全部开园，“三园协同、多点联动、辐射全国”的网络安全产业格局基本形成。2021年3月，国家网络安全产业园区（长沙）网络安全测试认证中心正式启用，标志着该园区“四中心”建设全部完成。截至2020年底，长沙网安园区集聚网络安全企业196家，三年共引进重点项目47个，总投资达625.4亿元。

二是网络安全创新应用先进示范区崭露头角。2020年11月，河南郑州、北京顺义、安徽合肥、重庆合川、江西鹰潭、浙江杭州六地的网络安全园区入选工信部“网络安全创新应用先进示范区”，各园区的专业特色水平和辐射带动作用已逐步显现。其中，郑州金水科教园区以内生安全为重点方向，先后签约20余家网络安全企业。重庆合川信息安全产业城已升级为重庆市网络安全产业园，目前产业规模总产值超过175亿元，并完成300亿元产业投资布局，计划与四川天府园区联合申报西部“国家网络安全产业园”。杭州市信息安全产业园已吸引国家级高新技术企业25家，落户园区的“5213”项目达到11个。

三是更多网络安全专业园区正在加速崛起。2020年10月，江苏骐谷科技产业园正式开园，这是江苏省首个以网络安全为主导产业的园区，已吸引29家企业入驻，2021年预计投资额250亿元。2021年4月，武汉市东西湖区国家网络安全基地一期核心区域展示中心、网安学院、培训中心等已投入使用，这是国内首个独具特色的“网络安全学院+创新产业谷”基地，注册企业已达120家，全国网安企业前50强悉数入驻。

4.人才培养多措并举深化改革

一是技能竞赛锤炼实战型安全人才队伍。2020年11月，“网鼎杯”网络安全大赛在深圳收官，大赛构造了覆盖十四大行业、六千多家单位的数字网络靶场，集结了来自全国各行业领域的14724支战队，共计50165人。2020年12月，全国电信和互联网行业网络安全管理职业技能竞赛在广州闭幕，历时4个月，覆盖全国31个省份，其中共有312名个人选手参加，106支参赛团队入围全国总决赛。二是网络安全企业赋能人才培养。2020年12月，安恒信息分别与浙江大学ArcLab实验室、黑龙江大学达成协议，助力大数据安全、云安全、物联网安全等领域技术突破，探索人才培养、人才就业新路径。2020年下半年到2021年，360分别与东北大学、天津职业大学等携手共建网络安全人才培养平台，通过深化培养方案、课程设置、教学内容、培养模式等内涵建设，打造网络安全人才培养体系。2021年4月，重庆大学、西南大学、重庆邮电大学等10所院校联合发起重庆市网络安全人才培养计划，奇安信将与院校在红蓝对抗、网络安全应急、网络安全运营等方向达成合作。三是人才培养基地打造网络安全高地。在国家层面，2020年9月，国家网安基地网络安全学院正式开学，超过1300名本硕博学生入驻学习；2021年3月，资助计划总金额达6000万元的“网络安全万人培训资助计划”启动，计划在未来三年内培养国家网络安全人才超过1万名。在地方层面，2020年9月以来，河南、沈阳、浙江等地网络安全科普教育基地和实训基地陆续落地，将在网络安全科普宣传、攻防演练、技术交流、技术实训等方面发挥重要作用。四是网络安全

大会汇聚行业智慧共话未来。2020年9月，国家网络安全宣传周在郑州盛大举行，吸引100余家互联网和网络安全知名企业参展，汇集1700余件网络安全领域最前沿的科技应用。2020年10月，网络安全大会“华山论剑”在西安顺利举办，会议聚焦5G、区块链、网络安全人才培养等热点领域，探索新形势下网络安全发展现状。2021年7月，互联网安全大会在北京开幕，会议包括近50场产业和技术分论坛、百余家线上线下融合展以及未来峰会、高峰论坛等特色活动。五是**在线培训成为安全教育新模式**。2021年4月，武汉国家安全教育网络基地正式上线，基地从总体国家安全观、国家安全动态、国家安全法律、国家安全知识等多个维度，通过文字、图片、体验式小游戏、影视作品、连环画和线上红色场馆等方式，创新网络安全宣教模式。

三、我国网络安全产业发展举措建议

总体来看，我国网络安全产业发展还处于高速增长初级阶段，与高质量发展要求相比，仍存在诸多问题。从市场发展来看，虽然产业规模稳步增长，但产业结构和发展质量有待提升，存在缺乏高端网络安全产品、安全服务发展滞后、产品服务与重点行业结合紧密度低等问题。从企业竞争力来看，我国头部企业营收、研发投入、技术水平与国际领先企业仍存在较大差距，国际市场业务难以突破，中小企业数量庞大但实力普遍偏弱。从产业生态来看，相关人才的缺乏、资本支持力度不足、安全意识及需求环境的不成熟成为制约网络安全技术创新和产业发展的重要因素。

2021年是“十四五”开局之年，数字经济迅猛发展，网络安全

迎来发展新的阶段。未来，我国应把握机遇，在完善网络安全政策体系、强化安全技术创新、优化安全人才结构、完善产业生态环境等方面持续发力，不断增强网络安全产业整体实力。

(一) 加速完善政策措施，筑牢网络安全坚实防线

为了护航制造强国、网络强国、数字中国建设，我国应不断强化国家战略的引领作用，加强在重点领域的网络安全战略部署和综合施策。一是加速出台顶层法律法规配套政策并推动落地。《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等基础性法律文件的相继发布，进一步完善了我国在数据安全、个人信息保护、关键信息基础设施安全保护领域的立法体系，同时为众多市场参与者提供了纲领性指引。下一步，相关法律落地实施的配套制度措施、标准规范应全面铺开，切实保障国家网络安全。二是持续增强对企业跨境上市的网络安全监管。为了应对跨境上市导致的数据安全风险，对于计划在国外上市的国内企业，要强化网络安全相关审查，进行更加严格的网络安全和数据安全管理。

(二) 持续强化技术创新，提升产业供给水平

在信息通信技术“数字产业化”和垂直行业应用“产业数字化”的双线驱动下，网络架构和应用场景都将发生巨大变化，为了应对新的安全威胁，应持续推动网络安全技术演进，不断完善产品体系。一方面，面向 5G、车联网、物联网、工业互联网等领域差异化需求，基础电信企业、设备制造商、自动化集成和应用服务提供商及安全企业应加强联合攻关，以应用场景为导向，以供给侧改革为着力点，

不断提升与业务的适配性，提高新型网络安全技术、产品、解决方案专业化水平。**另一方面**，在新威胁、新需求的牵引下，应持续追踪安全防护技术向智能联动、全面云化、系统化和实战化等方向的演变趋势，深化发展零信任、可信计算、拟态防御等新兴安全技术，逐步构建从底层防护引擎、威胁检测、安全探针等基础安全能力到上层场景运营、自动运维、安全服务等全面整体的网络安全防护体系。

(三) 不断优化素质结构，完善人才梯队建设

长期以来，网络安全人才数量与质量都不能满足产业发展需求，招人难、留人难、用人难一直是网络安全人才培养面临的最大问题。为了不断壮大人才队伍，应加速构建覆盖高等院校、职业院校、企业与社会机构、人才培养基地、公共服务平台等多层次的网络安全人才培养体系，加大创新型、技能型、实战型人才培养力度。此外，为了建设梯次合理、素质优良的网络安全人才队伍，应不断完善网络安全专业岗位人员持证上岗机制，通过逐步“淡化职称，强化职业资格”，全面提升人才队伍综合能力素质。

(四) 科学统筹要素资源，优化产业生态环境

为进一步优化网络安全产业结构，增强产业聚集效应，应加快构建网络安全产业发展良性环境。**一方面**，不断推进网络安全产业园建设，鼓励支持生态联盟、创新联合体等合作方式，强化网络安全产业的聚集效应，加速网络、人才、技术等资源要素的汇聚流动，激发更多创新活力。**另一方面**，随着提高供给质量、提升市场透明

度等需求日益迫切，应研究构建网络安全产品服务能力成熟度、质量评价等模型，部署开展基于新模型的能力评价，推动基于企业行为的信用体系建设，引导形成良性产业竞争环境。



中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62305321

传真：010-62300264

网址：www.caict.ac.cn

