中国数字安全产业年度报告

（2026）

公开版

（若需商业版请与数世咨询联系购买）

报告编委

首席分析师 **李少鹏**　　综合分析师 **刘宸宇**

战略分析师 **靳慧超**　　市场分析师 **闫志坤**

统计分析师 **牛爱民**

数世智库 **数字安全产业研究院**

版权声明

前　言

基于连续多年积累的产业调研能力和行业经验，经过大量的现场沟通、访谈，梳理、整理，统计工作之后，数世咨询分析师团队撰写完成《中国数字安全产业年度报告（2026）》，以客观地反映我国数字安全产业的真实状况，为国家主管部门、研究机构、行业用户，以及广大数字安全企业和相关从业者提供有价值的参考。

北京数字世界咨询有限公司

2026 年 6 月

目　录

第一章 数字安全九大态势

旧有的商业逻辑正在瓦解，而新的生态尚未完全成型。但也许正是这种极致的拉扯与试错，会倒逼安全产业开始去泡沫化，回归“解决实际问题”的原点。

—— 数世咨询 2026 年 6 月

第一章 数字安全九大态势

一、数字安全产业步入深水区

2021 年度，数字安全产业由高速增长阶段进入持续调整阶段。年复合增长率连续三年下滑累计达 30 个百分点，之后进入负增长阶段，市场规模连续三年缩水。以历史最高点 981.2 亿元（2020 年）计算，到 2025 年累计缩水近 100 亿元（2025 年为 887.43 亿元）。

外部大环境来看，全球经济疲软、政治与贸易冲突，以及人工智能带来的不确定性，均是国内数字安全产业发展困境的重要原因。内部自身来看，形式合规占据了整个市场的绝大部分需求，内卷式不良竞争挤压着彼此的经营空间，资源和资质的垄断则盘剥着民营企业的利润。合规既是产业的基础，却又成为发展的阻碍。

如何正确衡量安全的价值，形式合规如何转向实效合规，人工智能是机遇还是危机，安全产业健康发展的转型破局之路在何方？有无数个问题摆在每个安全人面前，需要求解、思考，验证和实践。至此，数字安全产业发展正式步入深水区。

二、产业碎片化格局愈加凸显

数世咨询在 2020 年的统计报告中指出，网络安全市场的格局为“只有诸侯，没有寡头”。到如今不仅没有形成寡头，碎片化格局却愈加凸显。

本报告统计显示，2025 年有 4 家企业营收在 30 亿元以上，占比 18.9%。11 家企业收入在 10 亿元至 30 亿元之间，占比 25.3%。20 家企业在 5 亿至 10 亿元之间，占比 14.5%；137 家企业在 1 亿至 5 亿元之间，占比 30.5%。

数字安全行业如此碎片化的本质原因有四：一是伴生属性。先有云计算、大数据、

人工智能，才有云安全、大数据安全和人工智能安全。同样，离开数字化，数字安全就无从谈起；二是服务属性。客户需要的是行业化、场景化、能力化，甚至是提供情绪价值的服务，而标准化的机器和“冰冷”的设备无法做到；三是信任属性。安全的核心手段围绕着信任展开，而信任是根据环境、对象和时间而变化的，因此需要不断地验证；四是对抗属性。没有最锋利的矛，也没有刺不穿的盾。“道高一尺，魔高一丈”是永恒的话题。这四大本质属性，前两者是被动的，后两者是动态的，四者交叉叠加，决定了数字安全行业的碎片化现状，并将永远碎片化下去。

三、政治、经济、数字化驱动安全

一般认为，发生安全事件和满足合规，是安全最大的两个驱动力。但这两种驱动力只停留在表面，因为实际上事件是可以发生的，只要事情瞒得住或责任甩得出。合规是可以不遵从的，只要无标准或做不到。数世咨询通过大量的访谈和调研，总结出安全需求的三大底层驱动力：政治、经济和数字化。

政治优先的党政军及央国企是安全的第一大需求方。数世咨询每年的行业统计，党政军、事业单位及央国企在安全上的采购要占到整个数字安全市场规模的 80%以上。从区域统计来看，央企总部集中的北京，仅这一座城市辖管的安全公司，总营收占到全国近一半的市场规模。

良好的经济发展是安全的第二大驱动力。无论哪个行业、领域，国企还是民企，雄厚的经营资金是足够安全预算的首要保证。不管是实际的用户访谈，还是乙方的调研反馈，有钱的用户在安全上的投入远超于同行，这已经是行业共识。一个相反的例子，前几年高增长的银行这两年步入低增速时代。在安全上的投入，已经连续四年下降。本报告对城市的统计同样显示，经济发达的城市，安全企业的集中度就会高。

第三大底层驱动力是数字化依赖程度。区域或机构的数字化依赖程度越高，安全

投入就越大。互联网就是企业数字化的代表，杭州、深圳就是城市数字化的代表。这些代表对数字安全的投入，远超其他同行和区域。

四、全行业减员并非 AI 之过

数世咨询统计，国内数字安全企业的从业人员在 2022 年达到历史最高点 14.7 万人，2025 年 11.72 万人，三年累计减少了三万人，全行业 20%的减员比例。与此同时，每家企业都在大谈 AI 赋能带来的效率提升，宣布 All in AI，甚至要用 AI 重构一切。再加上全球各领域都在讨论 AI 代替人的可能，于是至少安全领域的从业者，普遍认为 AI 浪潮将导致大规模减员，并且已经在现实中频频发生。但实际上这是一种错觉。

全行业 20%的减员是事实，但不是 AI 导致的。只要具体深入到每一家发生大规模裁员的企业，就会发现裁员的真正原因是经营压力，以三种最为典型的安全厂商为例：

第一种是规模较大的公司，只要发生大数量裁员，无一例外亏损严重。第二种是以融资续命或估值过高且造血能力差的公司，当资金无以为继的时候，一定会大规模裁员。第三种属于长期经营不善、积重难返的公司，濒临退市或倒闭，裁员已是必然。

有没有 AI 大幅度提升工作效率且经营良好，因此开始减员的公司？答案是，一家也没有。反而，这样的公司在不断地扩大员工规模。数字安全行业从业者的大范围减员，与其说是 AI 导致的，不如说 AI 是一个不错的借口。真正的根源在于经营压力和对未来的悲观预期。

AI 带来工作效率的提升毋庸置疑，但 AI 通过提升全社会生产力导致大规模社会减员，至少在现阶段还没有到来。

五、AI 浪潮下的焦虑与迷惘

身处人工智能巨浪中的安全产业，从监管到资本，从用户到厂商，从管理者到普通员工，焦虑与迷惘情绪无处不在。

监管机构一方面要鼓励产业迎接技术革命，另一方面又担心出现安全事故。投资机构一方面还在对过去几年的产业泡沫心有余悸，另一方面又在担心错失大好的投资机会。

绝大部分用户采购“无 AI 不立项”，令本来就捉襟见肘的安全预算被大幅挤压。而厂商即使将 AI 融入原有产品进行升级，但这部分成本大多只能自己负担。用户渴望通过 AI 实现降本增效，获取竞争优势。但与此同时，AI 带来的安全事件频出。厂商还未来得及做好 AI 安全产品和服务，监管已发文严控大模型和智能体在政企的使用。

不只是客户，大型安全公司本身也陷入了模型训练的“军备竞赛”，花费昂贵投入购买算力和数据治理，但并未换来预期效果。许多项目难以落地，许多公司陷入了投入与产出严重失衡的困境。虽然 AI 在研发和办公方面显著提升了效率，但企业的商业收入却未随之增长。效率的提升未能有效转化为商业价值，形成了“增产不增利”的尴尬局面。

旧有的商业逻辑正在瓦解，而新的生态尚未完全成型。但也许正是这种极致的拉扯与试错，倒逼安全产业开始去泡沫化，回归“解决实际问题”的原点。

六、安全垂域模型的两大挑战

业界呼吁安全垂域模型的声音已经很久，这两三年来安全大厂也先后推出了各自的安全大模型，虽然取得了一些不错的测评成绩，但在真实场景下的效果很难令用户满意。根源来自安全垂域模型的两大难题，一是缺乏用于微调的高质量安全数据，二是即使有了数据，也很难跟上基模的更新。

数据方面，虽然某些大厂手里有着海量的安全数据，但其并不等同于“高质量的

微调语料”。模型需要的是“当看到 A 日志和 B 流量组合时，说明攻击者正在进行 C 操作，因为 D 原理，所以我们应该采取 E 措施”的专家级推理文本。而将海量的流量、日志、样本转化为能让大模型理解的“专家经验语料”，需要成本极高的数据治理、人工专家标注和知识图谱构建。

基模方面，在人工智能技术与商业竞争激烈的当下，垂域模型所使用的基模更新升级频率极高。一旦基模迭代升级，一定与现有的软硬件系统冲突，需要对底层架构、算子或参数结构进行调整。而且，垂域模型都会有一整套的工程机制，如输出格式与校验、缓存策略等，基模更换意味着这些机制需要重新校准。模型迁移绝非简单的“接口替换”，而是一场涉及数据、算法与工程全链路的系统性重构。

唯有跨越高质量语料转化与基模系统性重构这两座大山，安全垂域模型才能走出测评的温室，在真实的业务场景中实现其应有的价值。

七、数据安全成第二生长曲线

自 2021 年开始，整个安全产业在历经多年高速增长后进入调整阶段，2023 至 2025 已经连续三年出现负增长。而数据安全领域，在整个安全产业规模不断下降的同时，呈现逆势且加速增长的趋势。2023 年的增长率仅为 3%，但随即就是 2024 年的 6.87%，2025 年的 11.11%。在整体数字安全产业受宏观预算收缩和传统产品同质化影响出现负增长的背景下，数据安全的逆势高增长具有深远的产业意义。

数据安全的连续增长其实并不意外，本质是因为网络安全的核心目的是数据安全，只不过由于我国数字化进程的阶段性特征，使得基础设施建设阶段的规模效应掩盖了这一本质属性。在基础设施红利消退、技术架构趋于稳定、数据要素红利分配开启后，这一本质才更清晰地显现。但值得注意的是，实现数据安全的基本手段是网络安全，两者只能从直接保护对象上做区分，在技术手段上是无法分开的。

在不破坏数据完整性的前提下，所有的数据安全技术和手段都是基于数据载体实现的，即网络安全。两者的结合即数字安全。——数世咨询

数据安全的增长将带领数字安全思路从外（边界）到内（流程）、从基础设施（网信系统）到数据（业务价值）进行转变，通过改变底层的技术逻辑和商业模式，有望重新定义产业的叙事逻辑。

八、利润第一重回商业本质

从数字安全行业从业人员和产业规模的比值来看，人均产出年年超过 65 万元甚至 70 万元，50%以上的毛利率十分普遍。表面上看是一个非常“赚钱”的行业，但实际上这几年全行业处于亏损状态。

如果仔细研究一下各家公司的财报，就会发现，销售、研发、管理费用耗尽了企业所有的利润。以本报告统计的 35 家上市公司为例，80%的数字安全上市公司销研管费用超过 50%，平均值则在 60%以上。意味着大部分上市公司的成本大于毛利。即便是未上市的公司，这种成本大于利润的情况也普遍存在。因此，近年来整个行业处于较为严重的亏损状态，也就不足为奇了。

积极的一面是，一些大厂已经开始减负，包括砍掉非核心业务或产线、拒绝亏本的安全服务、用利润而不是营收来考核销售。中小企业也纷纷将生存和赚钱放在第一位，而不是过去强调的规模和营收。只有当技术红利真正转化为企业利润，利润第一重回商业本质，数字安全产业健康发展的时代才会到来。

九、融资、上市、并购的痛点

自 2021 年近 170 亿元融资总额的历史最高点出现后，资本市场开始连续断崖式下跌。2022 年 100 亿，2023 年 39 亿元，2024 年 25 亿，2025 年 6 亿。民间资本

几近停滞。

自数世咨询提出“科创无望，北交拥堵，港交在望”的观点之后，到现在已有至少五家安全企业先后在港交所提交申请。在科创板改制落地之前，国资收购逻辑基本不通的情况下，港交所可能是资本仅有的退出路径。

最近几年，有不少投资人和创业者认为，既然上市走不通，并购一定是未来趋势。但实际情况并非如此。近几年来，除了两大运营商并购启明星辰与国盾量子以外，剩下十几起并购事件均呈现出并购金额小（千万级，甚至百万级）、以安全服务为主（典型的如各地的等保测评机构），以及大部分业绩对赌无法完成的三种特征，真正能实现 1+1>2 的健康并购案例可以说没有。

其中一个重要原因在于，国有资本极度谨慎，在考虑投资或并购时往往提出不能亏损、PE 估值、亿级规模和业绩对赌的四项基本原则。当下的经济环境，很难有企业满足所有这四项条件，而真正符合这些条件的企业则根本没有并购意愿。

最后，如果一份风险投资协议中充斥着刚性的回购、对赌，甚至于无限连带责任时，它已经不再是真正意义上的风险投资，徒有股权投资之名，但实际上成为另一种放贷形式。针对此现象，2026 年 6 月，国务院办公厅发布《关于加强监管防范风险促进私募投资基金高质量发展的指导意见》，首次明确将出台规范私募基金“对赌协议”的制度安排，并划定了明确的红线，“严禁明股实债”、“严禁脱离实际的无限连带担保”、“倡导柔性化解”。该文表明了国家层面在推动厘清股权投资本质，平衡投融资双方权责，引导私募基金回归风险共担、回归服务创新本源的态度。

毫无疑问，靠 PPT 讲故事、靠对赌协议博取高估值、盲目追求上市敲钟的“捂眼狂奔”时代已经结束。也许，阵痛过后，一个摒弃了资本泡沫、尊重商业常识，以价值回归为导向的数安新时代，正在缓缓拉开序幕。

第二章 数字安全·市场

综合国家政策大力推动、数字科技快速发展、数字安全重要性提升，以及当下政治经济形势等多种因素，2026 年将出现“震荡筑底”的态势。

—— 数世咨询 2026.6

第二章 数字安全·市场

一、市场规模

2025 年度，国内数字安全业务（含集成）总收入为 887.43 亿元[1]，相比 2024 年度（901.59 亿元）下降 1.5%。其中，数字安全集成业务收入 117.58 亿元，相比 2024 年度（113.77 亿元）上升 3%。

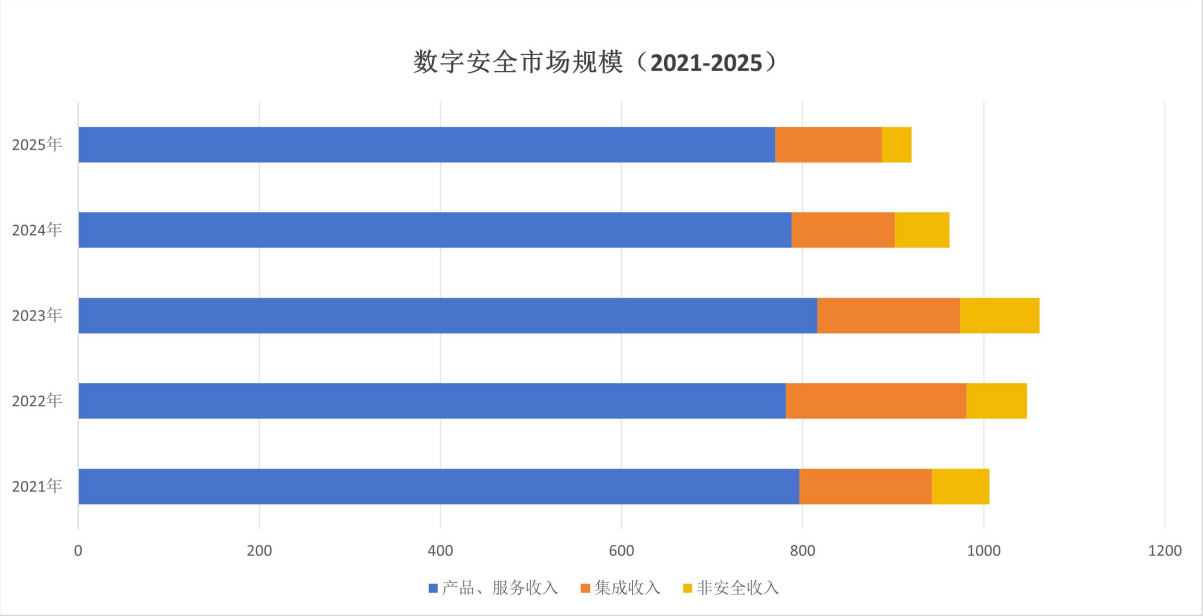


图 2-1 数字安全市场规模(2021-2025)

国内的数字安全市场规模从 2014 年伊始，进入高速增长模式。仅 2015 年至 2020 年的六年时间，市场规模逼近 800 亿元。而之前二十年的时间里，市场规模才达 240 亿元左右。

2020 年是历史增长率的最高点，亦是产业进入增长乏力期的转折点。从 2020 年增长率 29.9%开始下滑，2021 年 18.6%，2022 年 7.14%（市场规模达到历史最高 981.2 亿元）。2023 年首次出现负增长（-0.76%），2024 年负增长（-7.4%），

[1] *按照数世咨询的统计惯例，本报告将“数字安全业务（含集成）总收入”定义为默认语境下的数字安全市场规模*

2025 年负增长（-1.5%）。市场规模从 2022 年的历史最高点 981.2 亿元，连续 3 年下降到 2025 年的 887.43 亿元，缩水近百亿元之多。

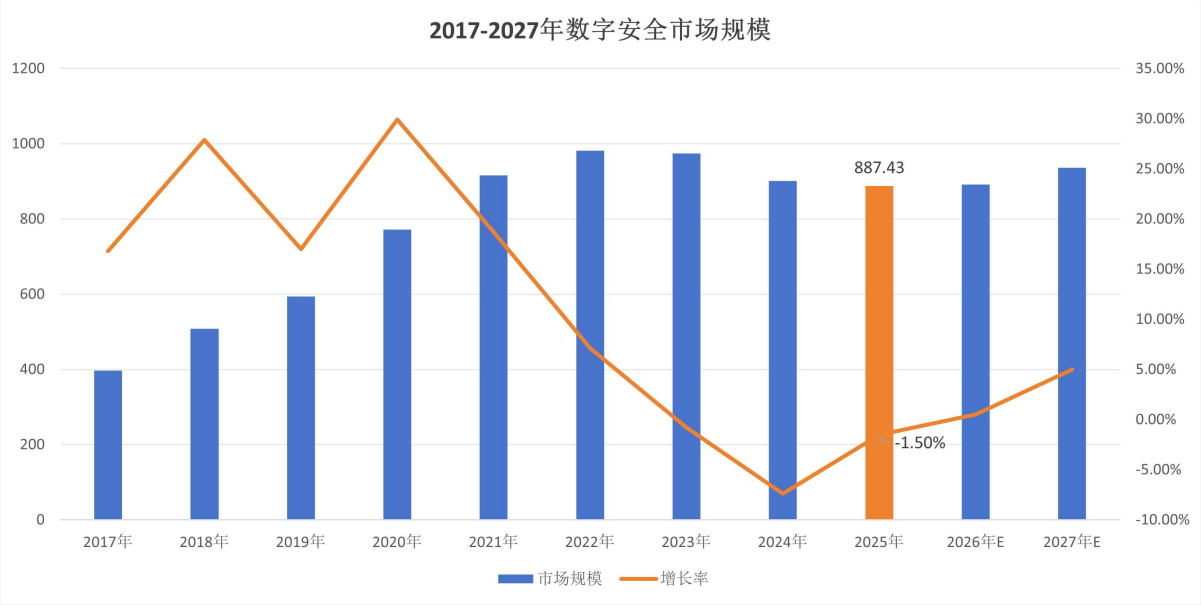


图 2-2 2017-2027 年数字安全市场规模

- **重要结论**

❖ 2025 年国内数字安全市场规模为 887.43 亿元，增长率为-1.5%。

❖ 市场规模的下滑态势从 2023 年的“微跌”，到 2024 年的“急跌”，再到 2025 年的“缓跌”。综合国家政策大力推动、数字科技快速发展、数字安全重要性提升，以及当下政治经济形势等多种因素，2026 年将出现“震荡筑底”的态势。

二、业务分类

依据数世咨询的统计惯例，将数字安全业务分为三大类：一是安全产品收入（含软硬件、设备及 SaaS 订阅收入）；二是安全服务收入（以人员投入计费为主）；三是安全集成收入。

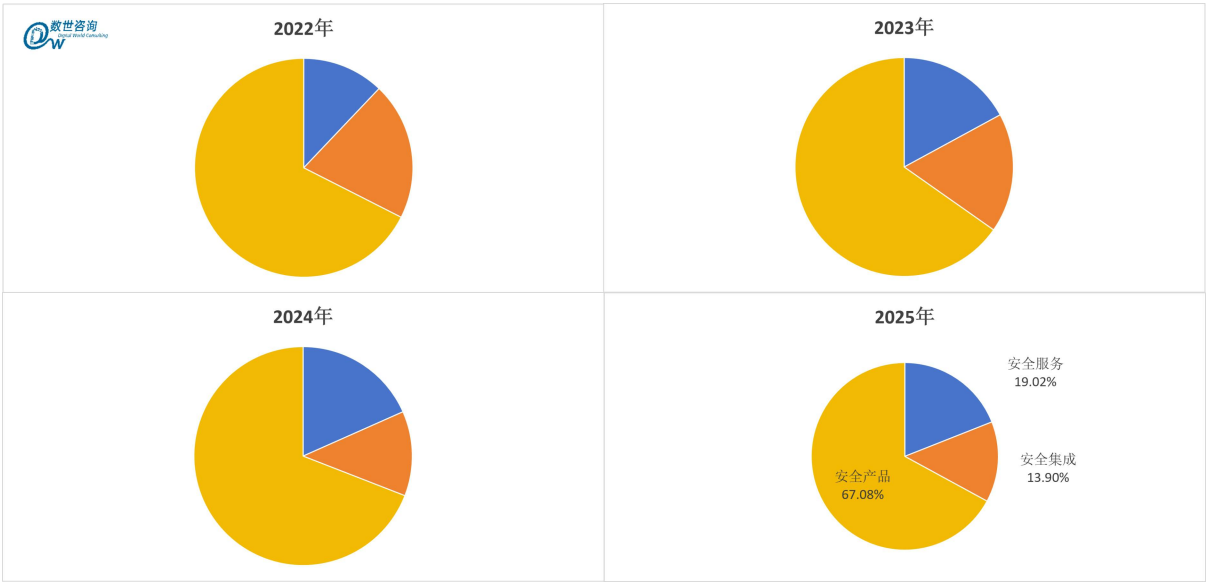


图 2-3 2022-2025 年 安全产品、安全服务、安全集成占比

- **重要结论**

❖ 2025 年，安全产品收入约占总收入的 67.08%，下降 2 个百分点，下降金额 27.2 亿元。

❖ 安全服务收入占比 18%，自 2021 年以来首次超过安全集成收入。

三、客户分布

根据本报告 400 家统计对象客户数据的不完全统计，将数字安全产业的核心客户群分为，政府部委、国家安全与公共安全、能源、运营商和金融等五大领域。

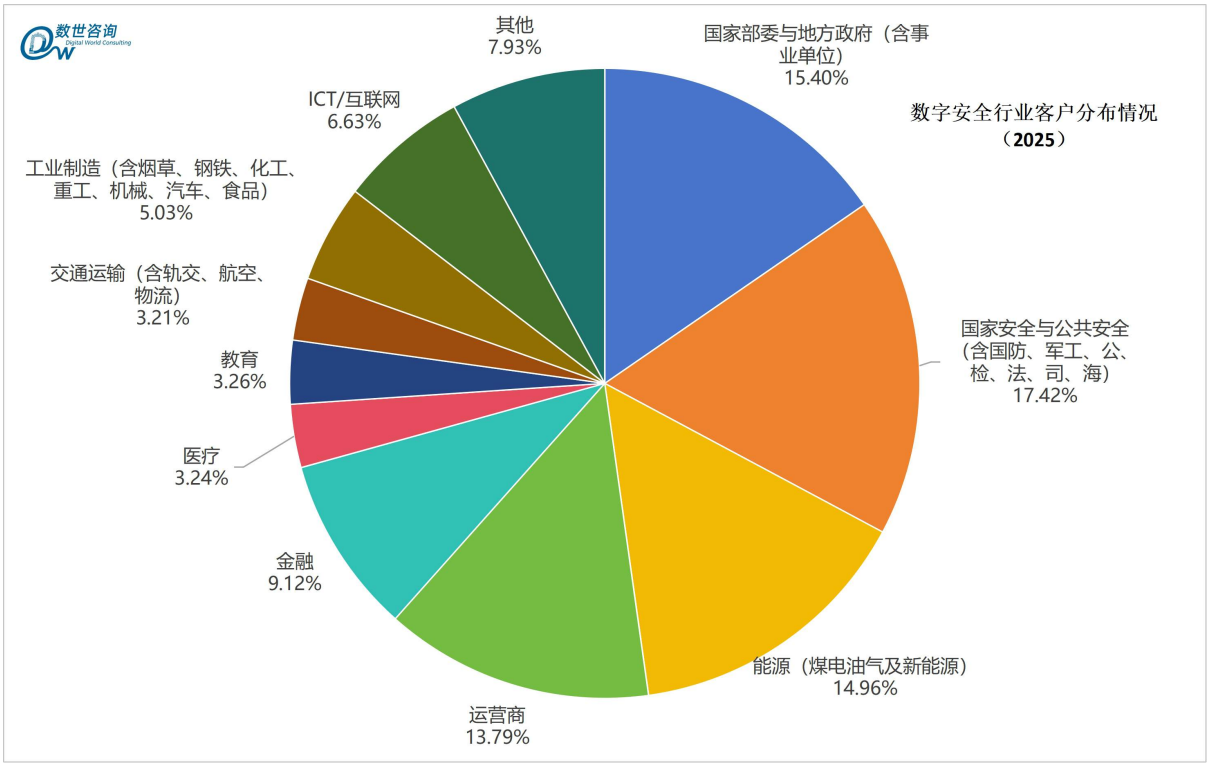


图 2-4 数字安全行业客户分布情况(2025)

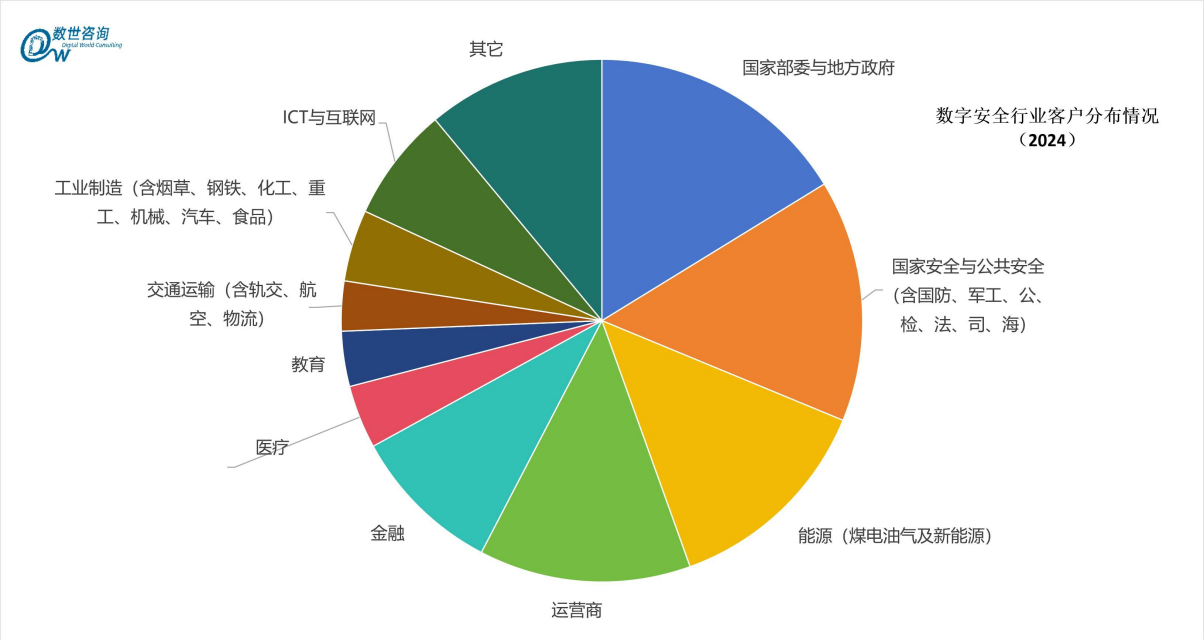


图 2-5 数字安全客户行业分布情况(2024)

- **重要结论**

❖ 安全企业在五大核心客户群的总收入为 588.34 亿元，占全行业收入的 70%。

❖ 行业需求方面，国防安全的占比首次超过政府部委上升为第一，能源、运营商、交通运输和工业制造的占比均有略升，金融、医疗、教育、互联网略降。这已是金融行业和政府部委的占比连续四年下降。

四、数字安全年度省份及城市

按照数字安全企业总部所在**省份**的安全行业营收（含非安全业务）排序，超过 20 亿元的有七个省份，分别为北京、广东、江苏、浙江、上海、四川、福建。（注：2024 年为八个省份，2025 年山东省因少于 20 亿元，因此未列入 2025 年的年度省份）

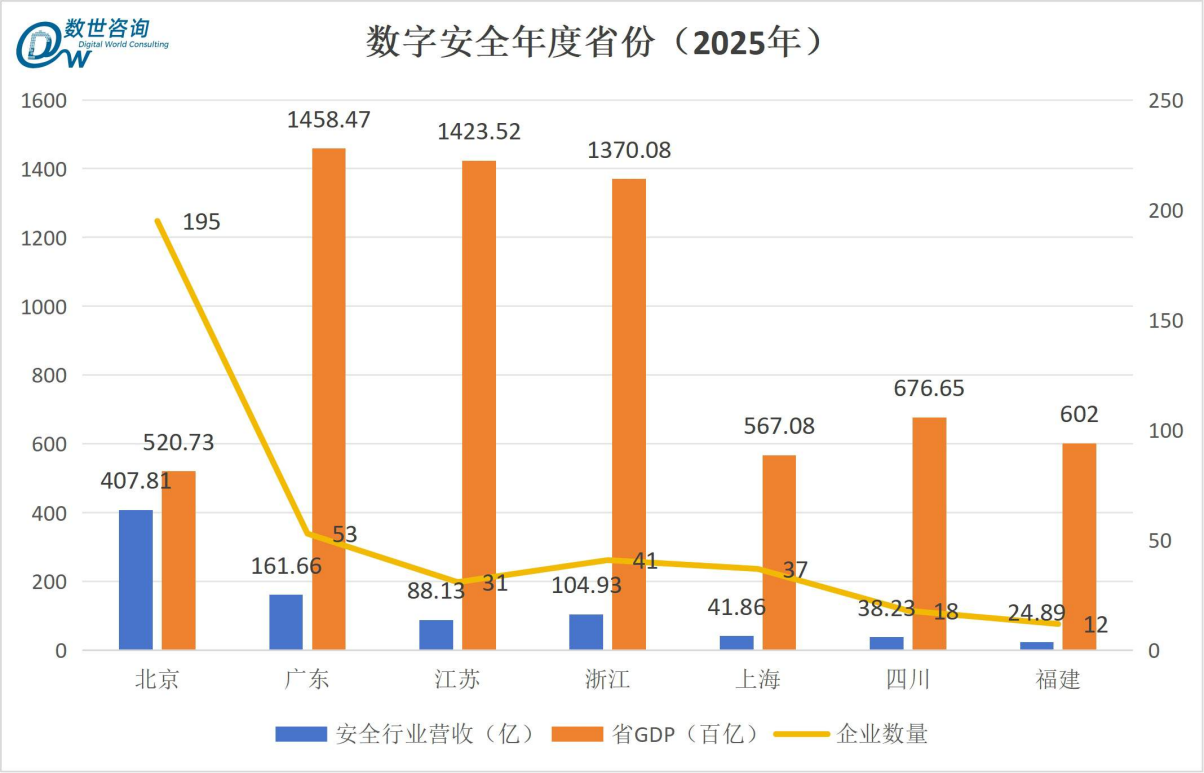


图 2-6 数字安全年度省份(2025)

按照数字安全企业总部所在**城市**的安全行业营收（含非安全业务）排序，超过 10 亿元的有十座城市，分别为北京、深圳、杭州、苏州、上海、南京、成都、广州、厦

门和济南[2]。

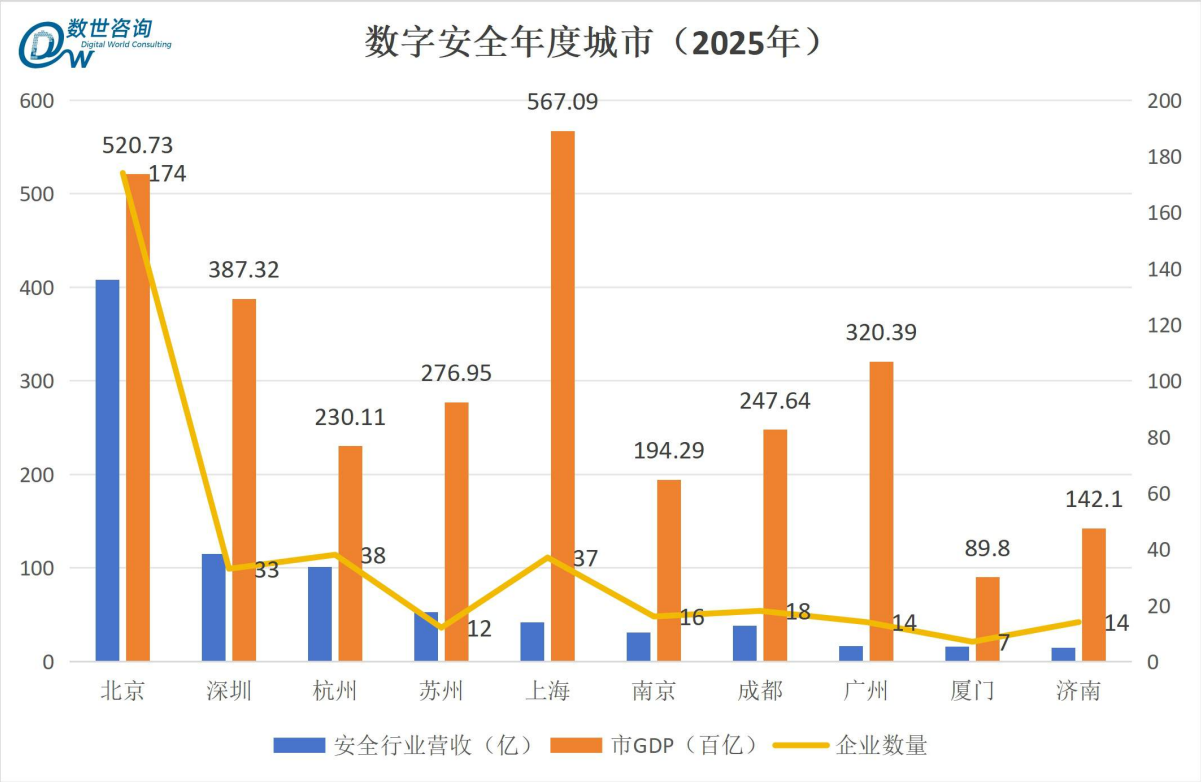


图 2-7 数字安全年度城市(2025)

- **重要结论**

❖ 从各城市数字安全企业收入占城市 GDP 的比例来看，北京和杭州最高，与该城市的 GDP 比值为千分之 7.8 和千分之 4.4。广州、上海最低，与该城市的 GDP 比值为万分之 5 和万分之 7。

❖ 按城市统计，仅北京一座城市的数字安全企业营收就占到十座城市总和的 48.8%（上年度 46%）。

❖

[2]因汕头市只有一家规模较大的数字安全企业，故未将汕头列入年度数字安全城市。

第三章 数字安全·企业

数世咨询在 2020 年的统计报告中指出，网络安全市场的格局为“只有诸侯，没有寡头”。现在来看，不仅没有形成寡头，碎片化程度反而愈加扩大。

—— 数世咨询 2026.6

第三章 数字安全·企业

一、营收水平

2025 年的数字安全业务（含集成）年收入，在本报告 400 余家统计对象中，有 4 家企业营收在 30 亿元以上，合计占比 18.9%。有 11 家企业收入在 10 亿至 30 亿元之间，合计占比 25.3%。20 家企业在 5 亿至 10 亿元之间，合计占比 14.5%；137 家企业在 1 亿至 5 亿元之间，合计占比 30.5%；228 家企业在 1 亿元以下，合计占比 10.8%。

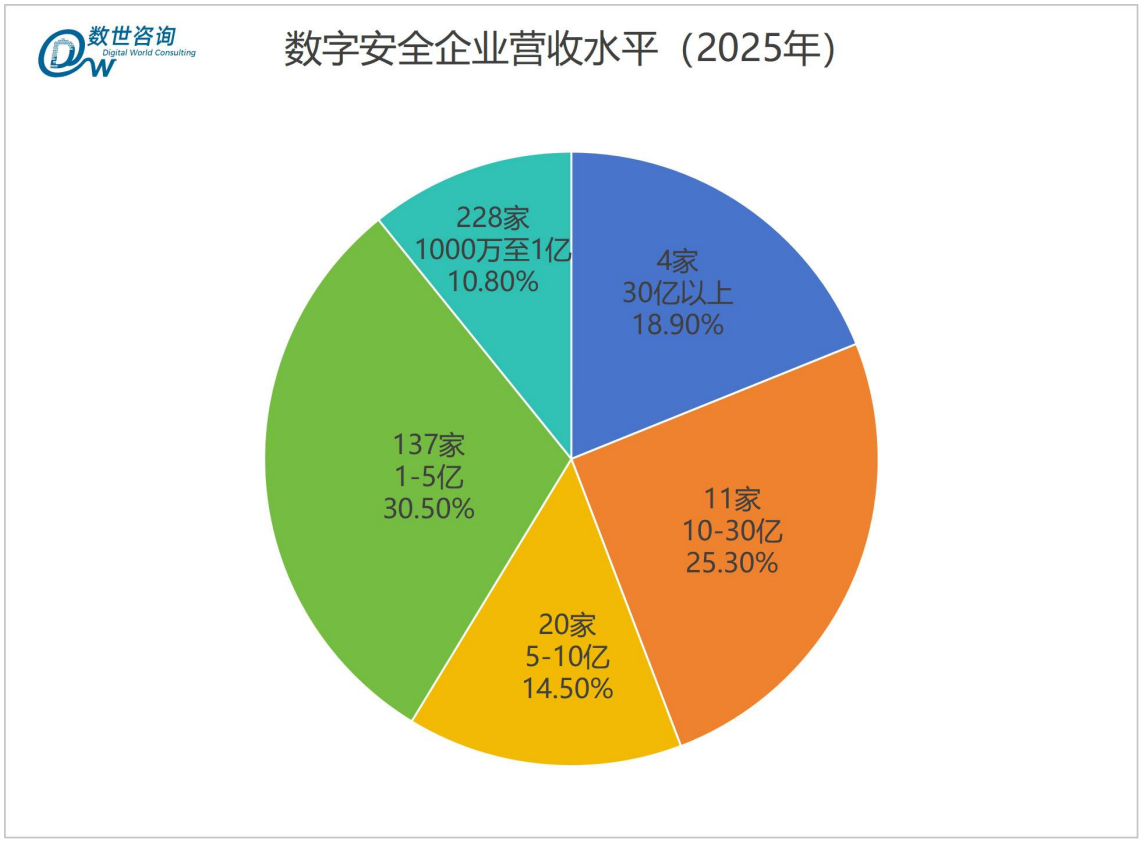


图 3-1 数字安全企业营收水平（2025）

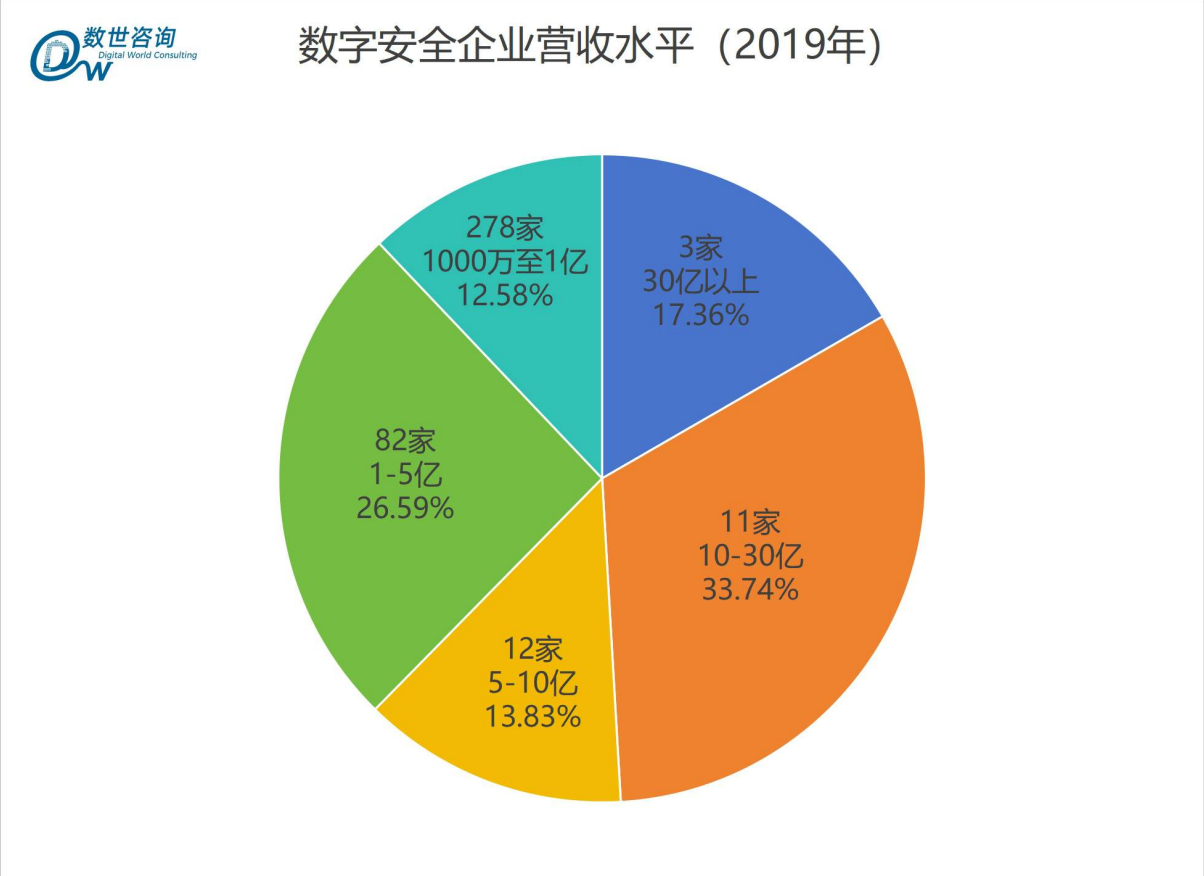


图 3-2 数字安全企业营收水平（2019）

- **重要结论**

❖ 数世咨询在 2020 年的统计报告中指出，网络安全市场的格局为“只有诸侯，没有寡头”。现在来看，不仅没有寡头，反而碎片化程度愈加凸显。

二、上市企业

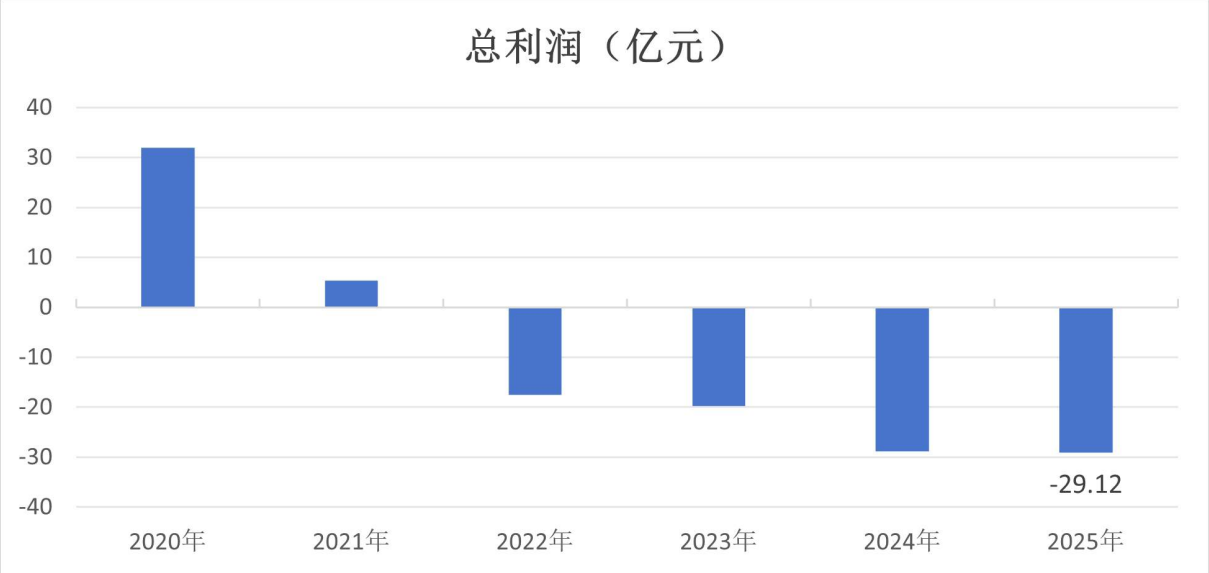
2025 年度，在沪深两大交易所上市的数字安全企业共有 35 家。（数世咨询定义的数字安全上市企业为，数字安全业务在总营收中占比大于等于 50%，或者绝对值超过 5 亿元人民币的企业）

2025 年沪深交易所的数字安全上市企业，安全业务总收入约为 339.68 亿元，与 2024 年（355.23 亿元）相比下降 15.55 亿元；净利润-29.12 亿元，与 2024 年（-28.89 亿元）相比，亏损增加 0.23 亿元；研发投入 93.8 亿元，与 2024 年（95.77 亿

元）相比下降 1.97 亿元；人均产值约 62.79 万元，较 2024 年（62.32 万元）上升 0.47 万元；员工总人数约为 5.41 万，较 2024 年（5.7 万人）减少 0.29 万人。

经营概况	2025	2024	增长率
安全业务总收入（亿元）	339.68	355.23	-4.4%
净利润（亿元）	-29.12	-28.9	-0.7%
研发投入（亿元）	93.8	95.77	-2%
人均产值（万元）	62.79	62.32	0.7%
员工人数（万人）	5.41	5.7	-0.5%

表 3-1[3]



[3]由于财报相关内容未披露，净利润统计不包括“三六零、亚信安全”，员工人数统计不包括“锐捷网络”，研发投入统计不包括“三六零、锐捷网络、亚信安全”。

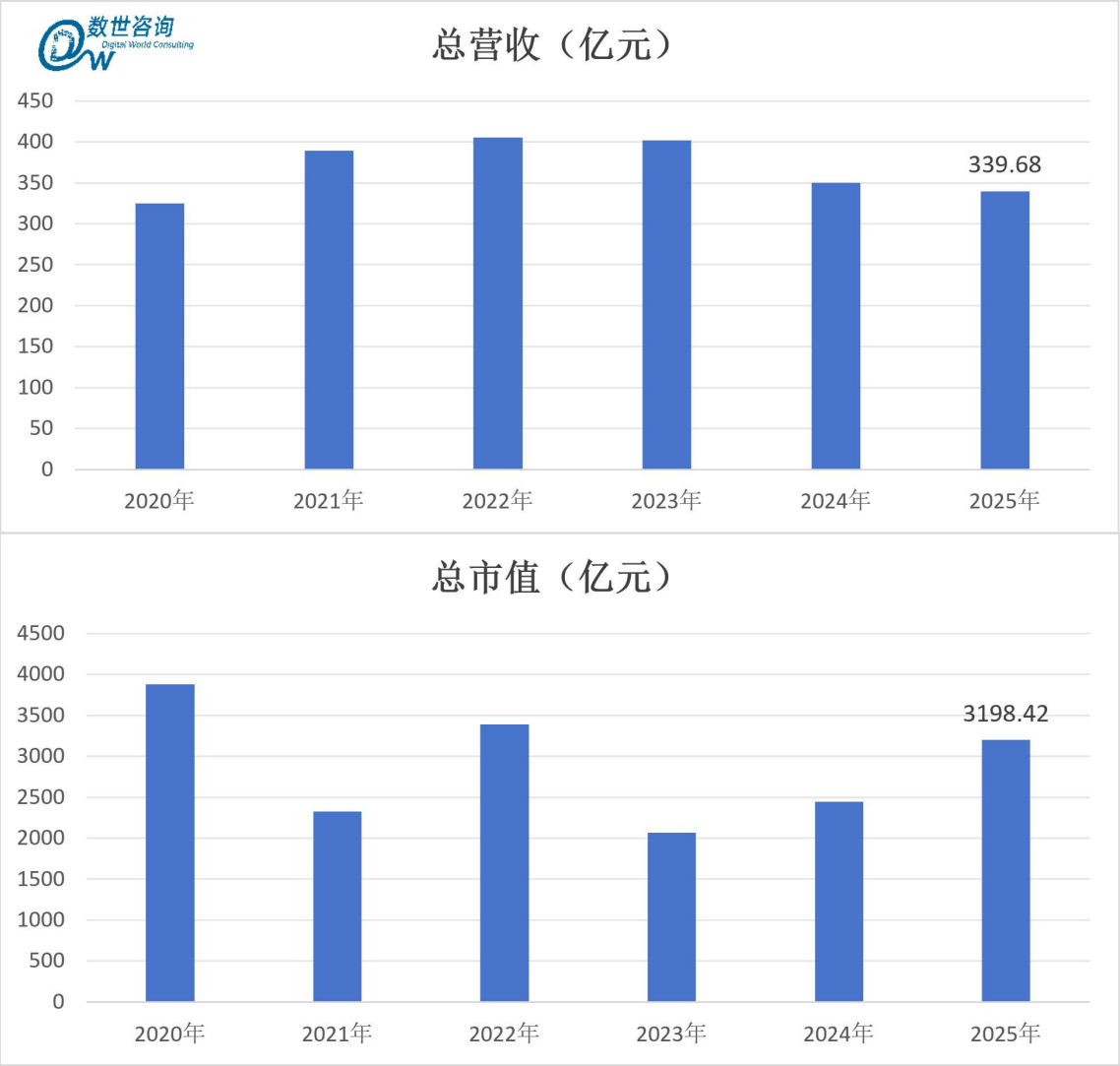


图 3-3 2020-2025 年数字安全上市企业三项指标

- **重要结论**

❖ 数字安全上市企业的利润、营收与人员数量均在微降，印证了《中国数字安全产业年度报告 2025》中“缓跌企稳”的态势预测。

三、新质·中国数字安全百强

2026 年 6 月 9 日，数世咨询正式发布《新质•中国数字安全百强(2026)》（以下简称百强报告）。

百强报告调研了国内 800 余家经营数字安全业务的企业，结合多种角度、不同维

度的企业相关数据进行梳理和评价。为突出新质生产力，更为公平地反映不同发展阶段的企业竞争力和创新力。

- **评价标准**

  横轴为企业发展力，主要考量经营能力、技术产品和人员文化三大类指标。

  竖轴为行业影响力，主要考量市场品牌、专业口碑和第三方评价三大类指标。

- **新质百强**

  新质百强（共 100 家），分为成长和综合两大板块，分别 50 家企业入选。

图 3-4 新质·中国数字安全百强-成长领域

成长领域为主营业务突出的企业，同时并未在 A 股或港股上市的企业。成长领域的基本入选条件为安全业务营收在 1 亿元以上。

图 3-5 新质·中国数字安全百强-综合领域

综合领域主要为 A 股或港股上市公司，以及一些包含安全业务的网络厂商、云服务商、软件集成商等规模较大的信息技术企业。综合领域的基础入选条件为安全业务营收 2 亿元以上。

- **年度成长力十强**

在数字安全产业持续下滑的态势下，那些业绩突出、逆势而长的企业，尤为可贵。以下是数世咨询评出的年度成长力十强企业：

图 3-6 年度成长力企业

四、新质·数字安全专精百强

国内许多未上市的中小规模企业，均在某细分市场或某区域有着专业化、精深化的创新优势，为了从不同维度凸显这些企业的优势，并与已经上市的企业分开赛道进行评价，数世咨询于 2026 年 6 月 15 日，首次正式发布一项新的企业榜单—《新质数字安全专精百强》（以下简称“专精百强”）。

专精百强中的企业，以产品、创新、区域、行业等四个版块展现，并分别注明由数世咨询定义的优势标签。

一、单项冠军

单项冠军是指，在某细分产品或服务上，无论是市场占比还是品牌影响力，均处于顶流的企业。且该细分产品与服务已形成基本成熟的赛道，包含多家相互竞争的企业。

二、创新之星

创新之星是指，该企业独立开发出一种新型产品或服务，并由第三方咨询机构通过真实调研，认可该企业为此类产品或服务的开拓者和引领方向者。

三、区域领军

区域领军有两个维度，一是在国内生产总值（2025 年）超万亿城市处于明显领先地位的企业，二是在某省份属于明显领先地位的企业。两个典型的特征，一是企业规模在本区域位于第一梯队，二是参与本区域几乎所有重要网络安全活动。

四、行业小龙头

行业小龙头是指，在某个大行业或细分行业，具备一流知名度的企业。且该企业的主营业务，经第三方咨询机构通过真实调研，认可该企业在同行业、同类竞品中的市场占比最高。

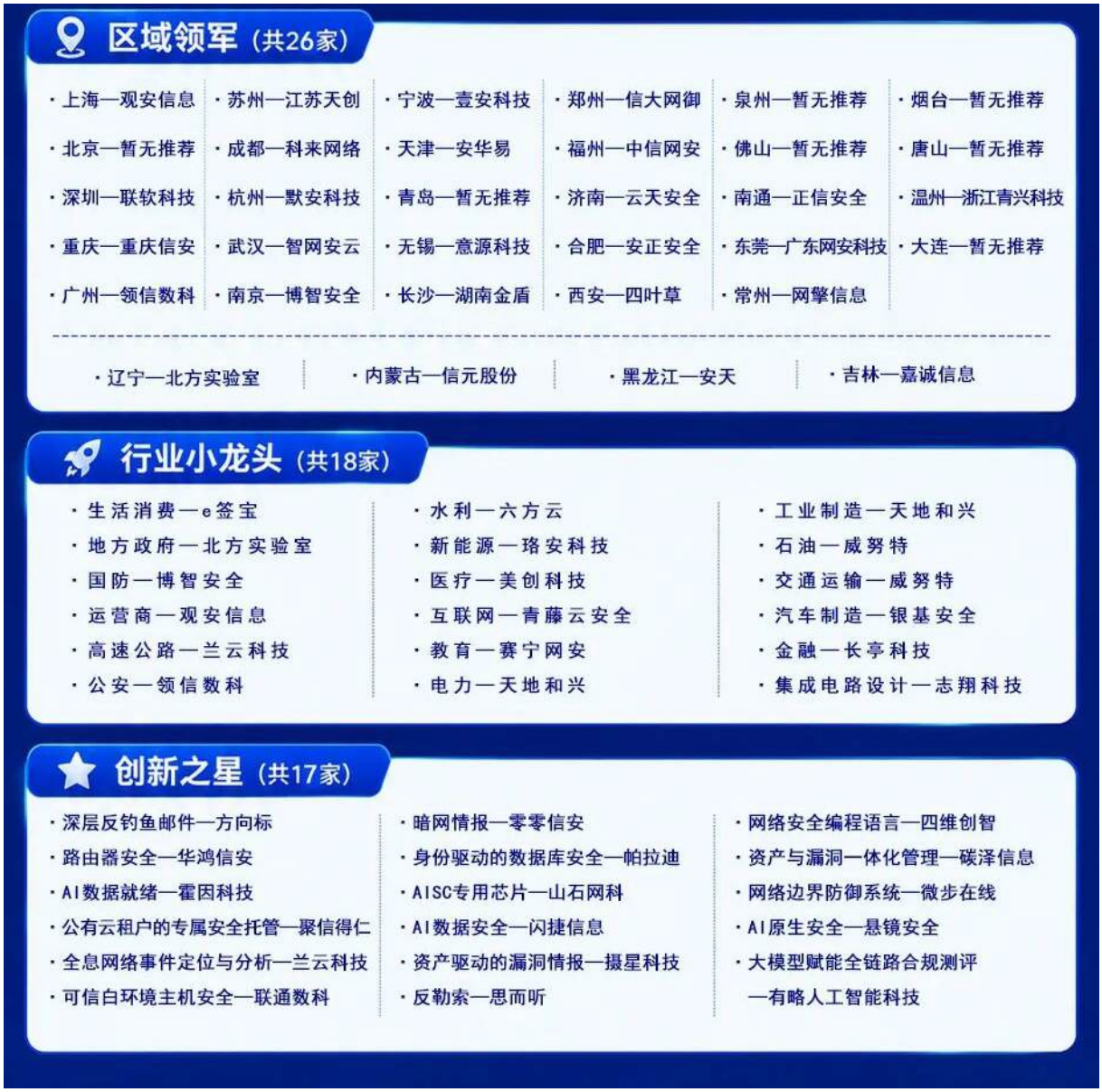


图 3-7 新质·数字安全专精百强

五、数据安全五十强

“中国数据安全 50 强”是数世咨询于 2024 年在业内首创的，评价数字安全产业中数据安全领域供应商的企业发展力和领域影响力的专业性评选活动，是继“中国数字安全百强”后的又一权威性产业榜单。

《中国数据安全 50 强调研报告》是该评选活动的成果，其根据大量、翔实的调研数据与访谈信息，从数据安全产品和服务的供给侧角度统计、整理、分析了上一年

度我国数据安全领域供应商的具体经营情况，并根据调研数据进行分析、得出洞察。

- **关键发现**

通过本次评选活动，根据全部调研数据并结合数世咨询对数字安全产业的洞察，有以下关键发现：

➢ **政策推进力度持续加大，数据安全认知更加清晰且深刻**

去年的 50 强报告中有一结论，即数据安全服务已成为先导性需求，历经一年后这一结论体现得更为明显。尤其是数据分类分级、数据安全风险评估两项服务，不论在合规亦或技术需求中都俨然成为一个共识，这不仅是技术上的必然，更是业务和合规的首要任务。

“不清楚保护对象，何谈保护”（数世咨询对网络安全的基础观点），这句话在数据安全领域更加切中要害。数据资产相比于网络资产更加庞杂与繁琐，混乱的资产管理只会增加风险面的暴露。不清楚数据流转的路径、共享的相关方、出境的内容风险，数据要素价值转化就是妄想。

数据安全风险评估不是简单的“漏洞扫描”，更不是“等保打勾”，而是为企业测量安全边界、测算价值转化的核心参考，数据安全风险评估的顺利推进，标志着企业对数据安全认知升级的必然结果。

➢ **数据安全呈现出高速增长，已经成为安全产业第二曲线**

自 2020 年开始，数字安全产业历经多年高速增长后急转直下，近年来更是呈现负增长现象。但与之相反的是，自数世咨询 2024 年开始单独统计数据安全领域以来，数据安全领域已实现 6.87%（2025）、11.11%（2026）的增长率。在整体数字安全产业受宏观预算收缩和传统产品同质化影响出现负增长的背景下，数据安全的逆势高增长具有深远的产业意义。

数据安全的连续增长其实并不意外，本质是因为数字安全的核心是数据安全（详见数世咨询数字安全三元论），只不过由于我国数字化进程的阶段性特征，使得基础设施建设阶段的规模效应掩盖了这一本质属性。在基础设施红利消退、技术架构趋于稳定、数据要素红利分配开启后，这一本质才更清晰地显现。

数据安全的增长将带领数字安全思路从外（边界）到内（流程）、从基础设施（网络架构）到数据（业务价值）进行转变，通过改变底层的技术逻辑和商业模式，有望重新定义产业的叙事逻辑。

- **数据安全的需求渐次明朗，实现业务增量是其核心归宿**

从大量的数据安全项目中不难发现，在中大型企业或项目中，以数据治理、数据流通、数据共享为目标的数据安全需求集中凸显，这也契合了数世咨询对数据安全的本质洞察，数据即业务、数据安全即业务安全。

虽然我国的信息化已跃然升级成为数字中国的新形态，但其实并未完全改变我国数字化程度阶梯形状态的本质，行业间的数字化应用程度甚至可达“天壤之别”。由于绝大部分行业并没有完成良好的数字化转型，但又由于国家对数字化改革的坚定意志以及数据要素价值转化的确定性，巨量的企业将数据治理、数据流通、数据共享等业务的推进又排上了日程并且增加了优先级。

在业务增量的逻辑下，企业已经不需要讨论是否做数据安全，而是需要专注于如何平衡监管政策、如何通过适合的技术与管理手段，去逐渐撬动原本无法触及的业务增量。

- **AI 发展延伸新的风险边界，数据安全呈现内外双重驱动**

在数据安全自身的增长逻辑之外，由于 AI 应用的迅速普及，针对 AI 训练数据、AI 合成数据、大模型输出数据（包括信息）以及业务 Agent 所触及的业务数据、个

人信息等方面的数据安全风险呈指数级上涨，使得 AI 数据安全已经成为强势且稳定的外部驱动力。

全球 AI 竞争已经从基础模型、设施的争夺进入了 AI 应用落地与商业变现的决胜期，而“AI 有用”靠的是业务流程再造与数据流通。当有价值的数据直接被 AI 使用时，对于数据的安全保障能力将迎来有史以来最大的考验。

当 AI 摇身一变成为数字员工时，AI 数据安全风险将对传统安全保障能力形成降维打击。因为过去 30 年的安全思路都是围绕着结构性数据流和可预测的软件行为设计的，而 AI 由于其黑盒特性与强大的关联能力，正与这两点背道而驰。目前的 AI 数据安全完全滞后于新型的攻击手段，只能依靠“亡羊补牢”的应急响应。

AI 应用的发展需要稳定性、AI 应用的价值在于高效性，而这一切的前提是安全性。AI 已经从科技争夺上升为国家竞争，而 AI 安全可能成为左右格局的最大变量。这不仅是我国数字安全产业的挑战，更是百年一遇的巨大机遇。

- **评选背景**

自 1994 年国务院第 147 号令（计算机信息系统安全保护条例）发布以来，随着经济与社会的发展，数字安全产业的核心关注历经了不同阶段，从计算机信息系统安全延伸到信息安全、最终扩展到网络空间安全。

伴随着全球数字化的脚步，网络虚拟空间与现实物理空间的关系越来越紧密、界限越来越模糊，数字中国概念应运而生。自此，网络空间安全从理念上升级为数字安全，核心目标是有效维持数字世界与物理世界的映射的全方位安全状态、维护数字秩序，并为有效维持物理世界的安全状态、保障国家安全提供核心支撑。

数字安全主要通过物理安全、网络安全和数据安全（包括信息安全）提供技术控制手段。我国法律明确指出，受保护的数据主要分为网络数据、关键业务数据、涉密

数据、个人信息 4 类，本报告所描述的数据仅指网络数据以及其他 3 类中的电子数据。由于数据要素战略的推进，数据所蕴含的价值和迸发的能量正在逐渐显现，加之智能化的确定性未来，又进一步证实了数据要素战略的前瞻性与正确性。

任何事物的风险都与其价值成正比，数据也不例外。由于数据安全在社会和经济发展中的重要性愈发凸显，数据安全产业也显现出技术与规模双双高速增长的趋势。

为了推动数据安全领域健康发展并搭建数据安全供需双方的沟通渠道，数世咨询于 2024 年在业内首创“中国数据安全 50 强”榜单。希望通过持续调研过程，可以向需求方推荐优秀的数据安全供应商，为供给方提供可转化的数据安全商机，共同构建可持续发展的健康产业生态环境。

- **评选结果**

据数世咨询统计，具有数据安全业务的数字安全供应商大约 500 家。本次评选中，根据综合得分，评选出专业实力 26 名，综合实力 24 名，两类共 50 名。

“中国数据安全 50 强（2026）”榜单如下图所示。

图 3-8 中国数据安全 50 强-专业实力

图 3-9 中国数据安全 50 强-综合实力

- **调研分析**

2025 年度，我国数据安全领域市场规模达到 68.91 亿元（开票额），较 2024 年度增长 6.89 亿元，增长率为 11.11%。

其中专业实力类市场规模为 27.12 亿元，增长 3.44 亿元，增长率为 14.53%。综合实力类市场规模为 41.79 亿元，增长 3.45 亿元，增长率为 8.98%。

图 3-10 数据安全市场规模及增长预测

据去年 50 强报告预测，2025 年度数据安全规模为 69.5 亿元，基本与今年实际情况一致，代表着数据安全领域的预期与实际情况未发生变化，持续向好，进一步夯实了数据安全领域在数字安全产业的引领带动地位。

注：以上预测是在数据安全以及数据安全供应商、数据安全产品的定义和范围（详见统计标准）不发生变化的情况下得出的，仅供参考。

在行业营收方面，运营商第一，金融第二，政府部委第三。前三名占有率为 40%左右，与去年相比降低约 2%，基本保持一致。

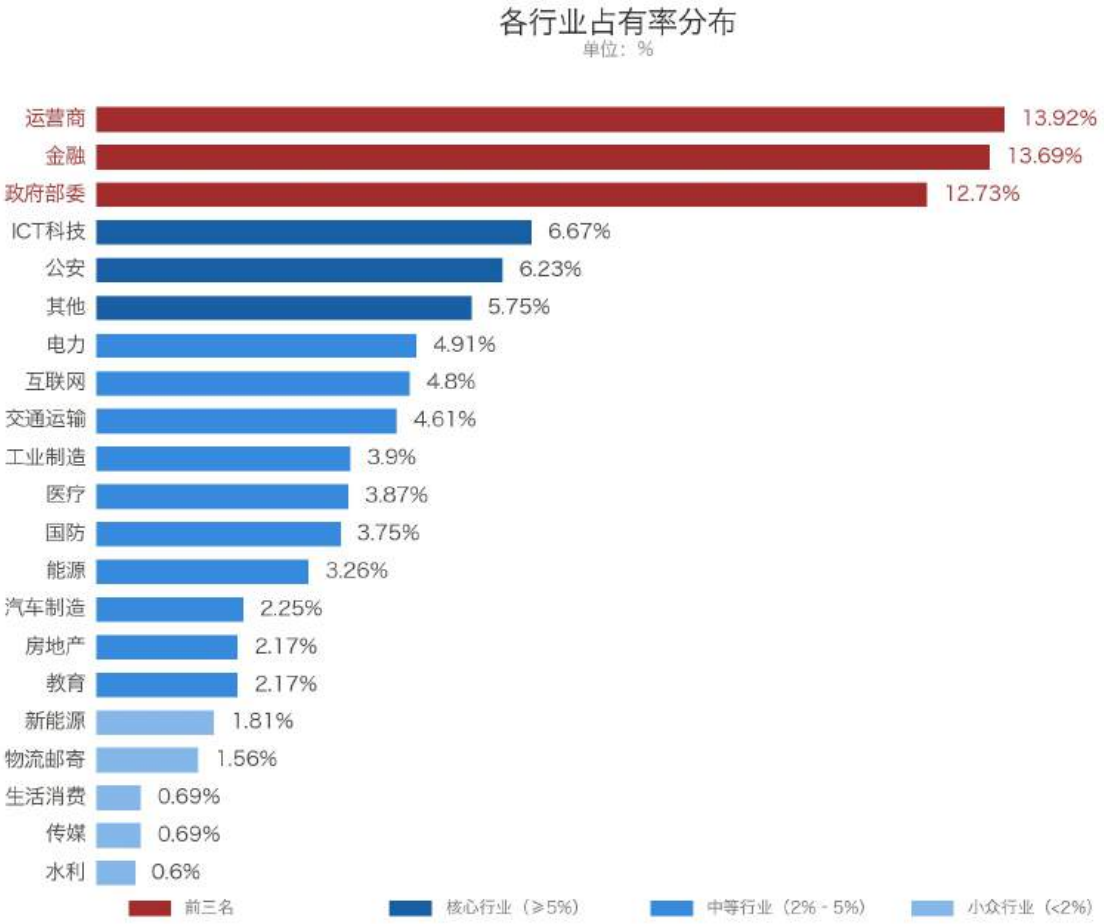


图 3-11 各行业占用率分布

在区域营收方面，华北第一，华东第二。前两名占有率为 60%左右，与去年相比降低约 2%，基本保持一致。

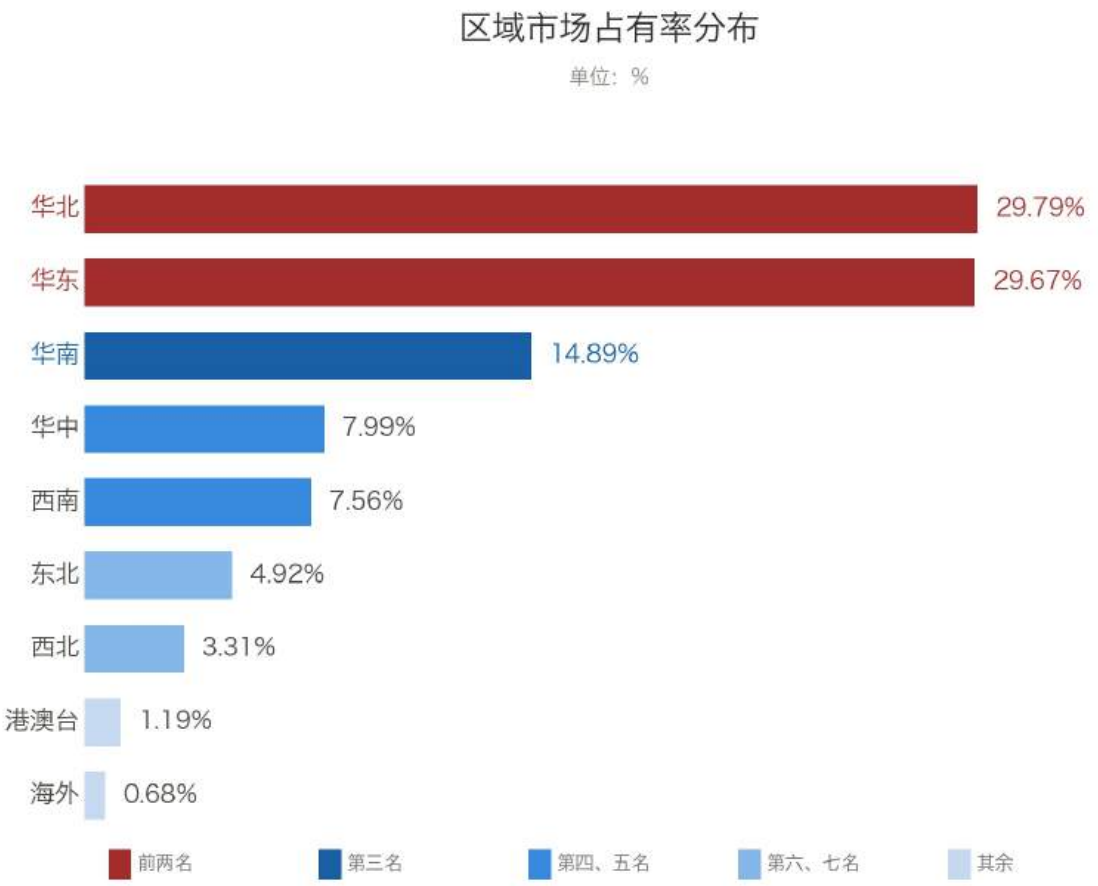


图 3-12 区域市场占用率分布

六、从业人员

2025 年数字安全企业从业人员约 11.72 万，较上年度下降 6.4%。其中技术人员 7.38 万人，约占 63%。

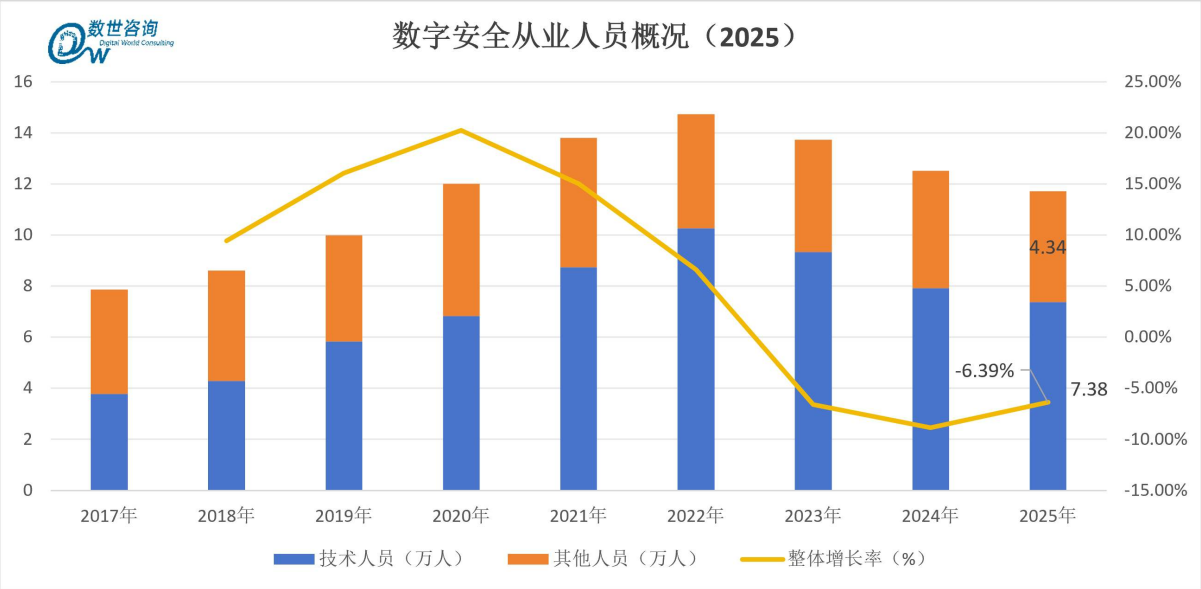


图 3-13 数字安全企业人员概况

第四章 数字安全·技术

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展的政策法规、管理措施、技术方法等安全手段的总和。

—— 数世咨询 2022 年 6 月

第四章 数字安全·技术

一、数世价值论

自数世咨询在 2022 年对数字安全做出概念性的定义之后，ChatGPT 于年底问世，并开启了新一轮人工智能的浪潮。2023 年百模大战，2024 年 DeepSeek，2025 年氛围编程，2026 年龙虾智能体。在此背景下，数世咨询将数字安全三元论迭代升级为数字世界价值论，简称数世价值论（Digital World Axiology）。

支撑价值论的模型为三棱锥架构，由数字活动、数字资产、数字安全和人工智能四个支点构成轮廓，数据充满整个架构。

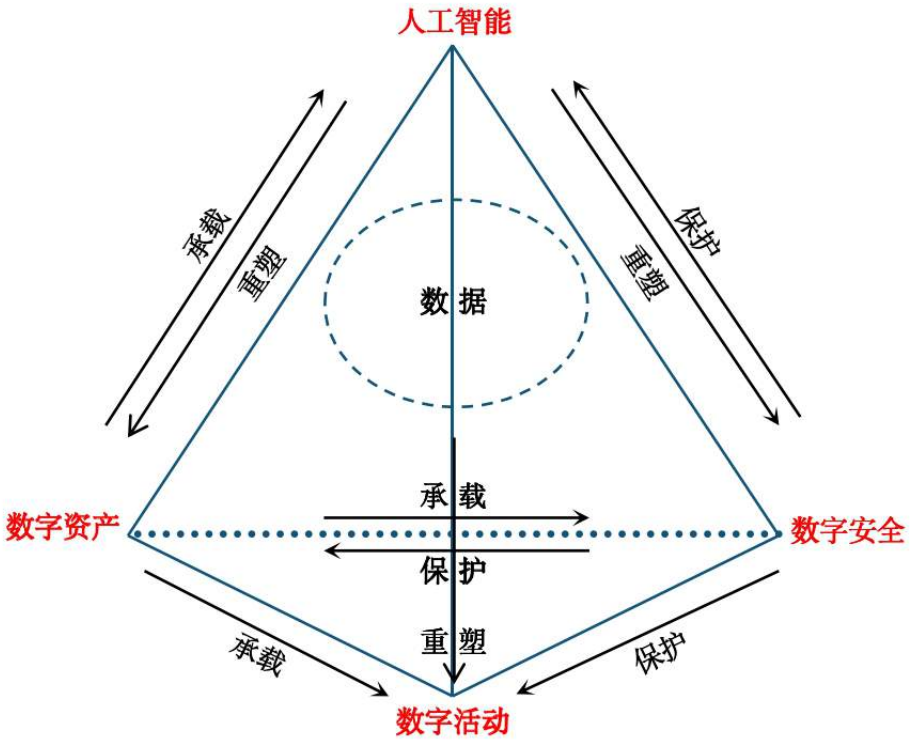


图 4-1 数世价值论

- **组成部分**

1.数字活动（Digital Business）：个人或组织持续进行的一系列数字化行为、操

作和流程的总和，是一个动态的、价值创造的过程。

2.数字资产（Digital Assets）：由信息基础设施和应用系统组成，是数字活动的载体。

3.数字安全（Digital Security）：以价值守护为目标，所需的数字化风险应对能力的总和。

4.人工智能（Artificial Intelligence）：突破人类智能极限，实现价值跃迁的革命性科技。

- **相互关系**

1.数字资产对于其他三点的作用为承载。

2.数字安全对于其他三点的作用为保护。

3.人工智能对于其他三点的作用为重塑。

4.数字活动是其三点的共同目的。

数世价值论（DWA）是一个由数字活动、数字资产、数字安全和人工智能四大核心要素构成的理论框架。其中，数字活动作为个人或组织持续进行的数字化行为与操作，是动态的价值创造过程，同时也是其他三个要素的共同目的。数字资产作为数字活动的载体，对其他三点发挥着基础承载作用。数字安全以价值守护为目标，提供应对数字化风险的能力，对其他三点起到关键的保护作用。而人工智能作为突破人类智能极限的革命性科技，则对其他三点产生深刻的重塑作用。这四大要素相互协同，共同构建了一个以价值创造为导向、以资产为承载、安全为保障、以人工智能为引擎的数字世界发展新范式。

二、数字安全价值图谱

图 4-2 价值图谱

1. 主流产品

主流产品是指市场普及率高、已得到广泛使用的标准化产品，如等保要求的大部分产品。

图 4-3 价值图谱-主流产品

2. 业务场景

业务场景是指以甲方工作（业务）需求视角提出的安全解决方案，不包括可以明确提出产品名称的采购要求。

图 4-4 价值图谱-业务场景

3. 合规场景

合规场景是指为了满足合规检查为目的的解决方案。

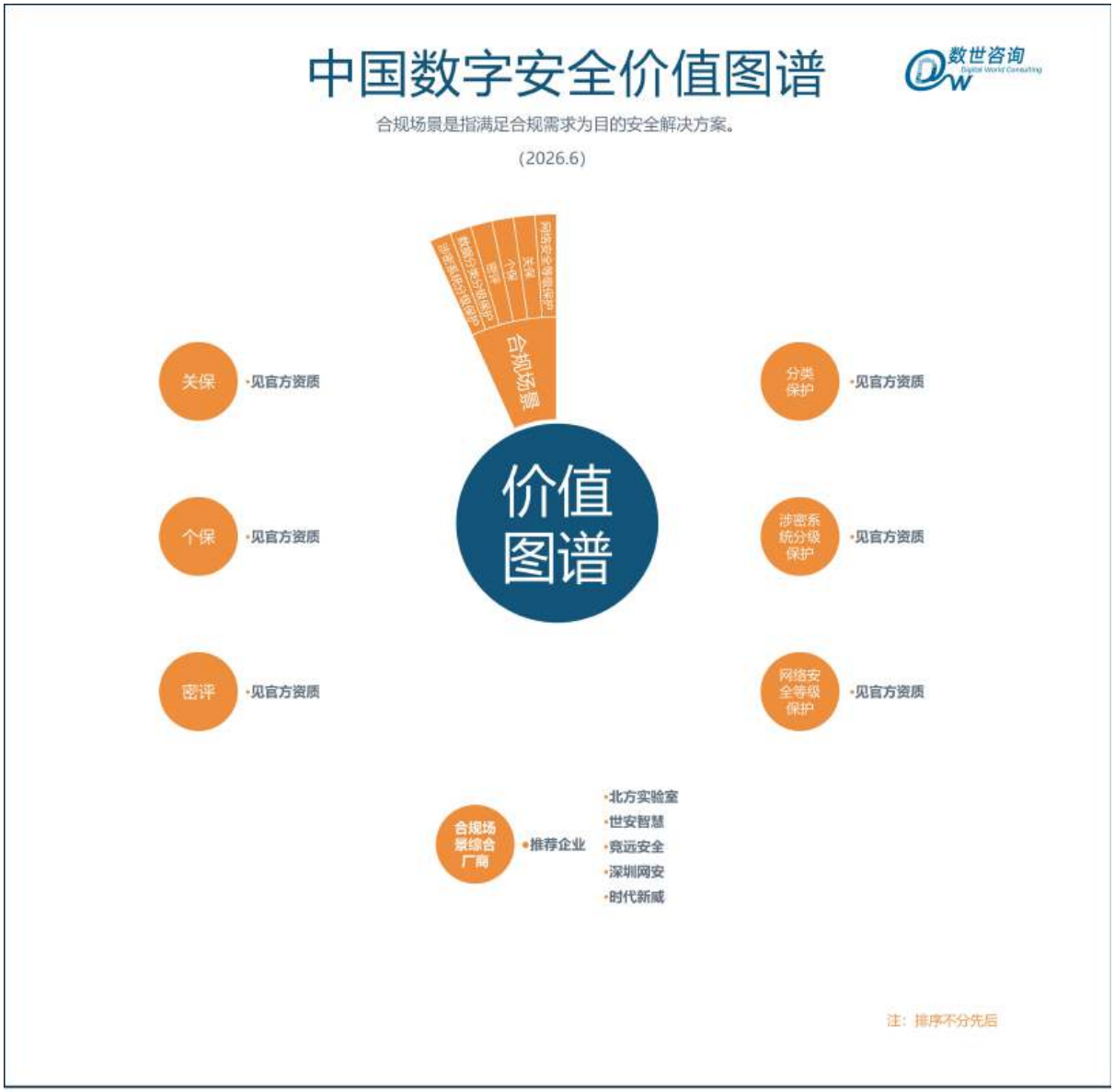


图 4-5 合规场景

4. 资产保护

资产保护场景是以具体的信息资产为保护对象，如容器、终端、数据库、网络等。

图 4-6 价值图谱-资产保护

5. 生态产品

生态产品是指为网络安全技术、产品赋能的工具类产品。

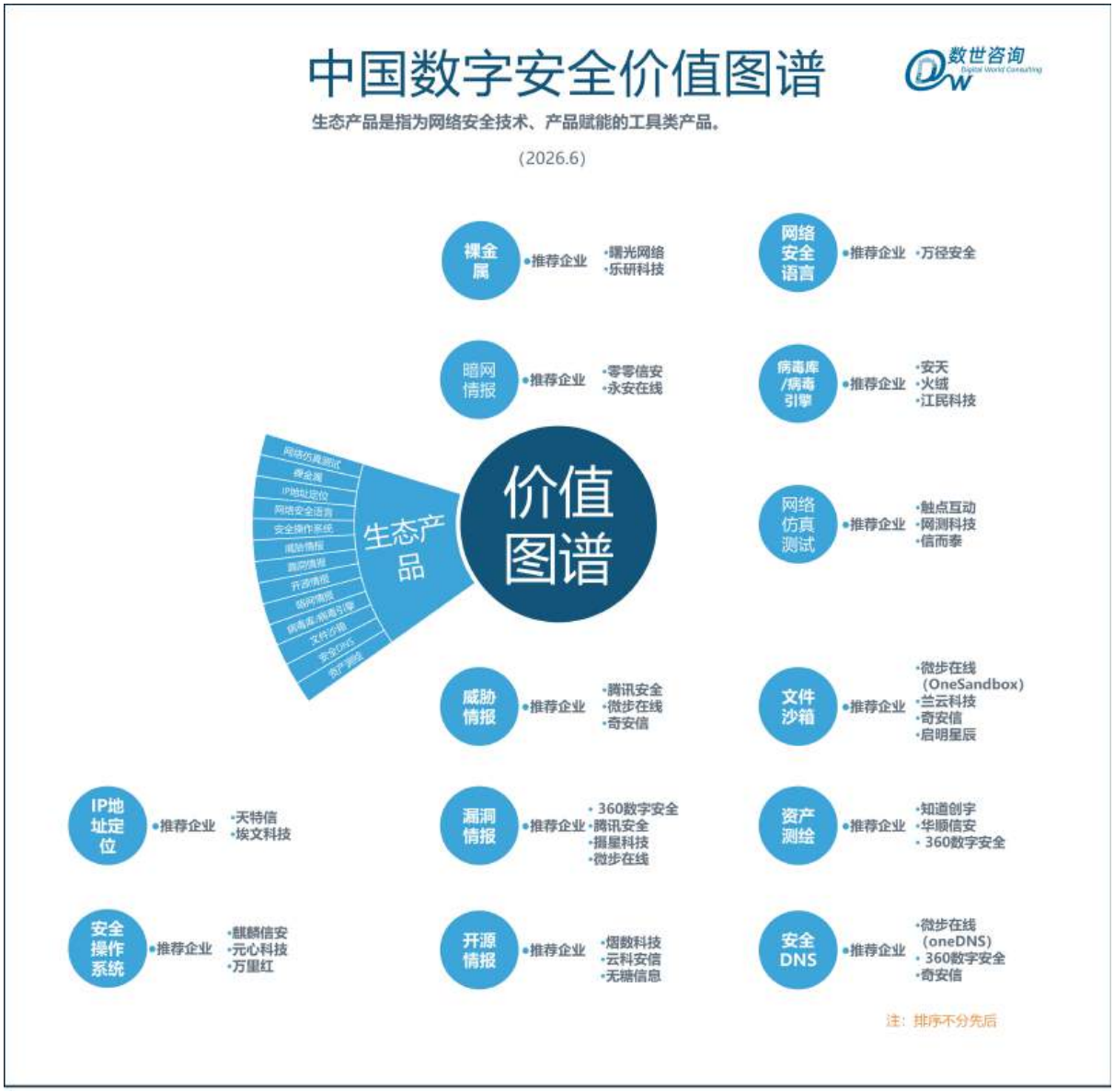


图 4-7 价值图谱-生态产品

价值图谱基于价值理念，以核心能力为核心，甄选出了细分领域市场占有率较高或技术创新性较强的供应商，凸显优秀安全能力提供者，降低供需双方的试错成本，为广大数字安全领域的业界同仁提供研究借鉴与参考。

三、年度创新赛道

数字安全是一个多维度、多场景，且不断动态变化的领域。因此，即使是在经济疲软、产业不振的大背景下，依然不断地有创新者出现。以下是数字世咨询与这些创

新企业共同打造的创新赛道：

1、创新赛道：AI 原生安全

领航者：安普诺（悬镜安全）

作为数字供应链安全领航者，悬镜安全基于“智能情报驱动，以 AI 治理 AI”核心技术理念，持续构建融合软件供应链安全与 AI 原生安全的新一代数字供应链安全治理体系，其首创新一代 AI 原生安全治理体系，从供应链源头治理 AI 智能体全生命周期原生安全风险。

AI Coding 安全：灵脉 AI 智能体，依托 AI 代码漏挖、AI 代码护栏与 SAST 审计等关键技术，将安全分析与智能修复能力进一步前置，精准挖掘深层漏洞，确保 AI Coding 源头可信。

AI 智能体安全：问境 AIST 智能体，依托原创多模态 AIST 技术，以 AI 评估 AI，通过 Skills 安全审查、AI 智能体审计、AI 红队测试与 AI 模型扫描等关键技术，精准识别模型投毒等 AI 原生威胁。

AI 供应链安全情报：悬镜首创 AI 安全情报订阅服务，聚焦数字供应链源头未知漏洞与投毒风险，实时提供小时级 AI 安全情报预警与极速响应服务。整体误报率精准控制在 3% 以内，让企业彻底告别“被动响应疲劳”。

作为以 37% 市场份额持续领跑数字供应链安全的行业标杆，悬镜安全具备极强的产品服务落地交付能力，已广泛服务金融、能源、大制造、运营商等重点行业 KA 客户。

2、创新赛道：AI 数据就绪

领航者：霍因科技

AI 数据就绪（AI Ready Data），霍因科技深耕 AI 数据落地赛道，直击企业 AI 产业化落地核心痛点。依托网信办合规备案的自研数据加工大模型矩阵（3B/7B/14B/32B 全参数覆盖），打破传统 AI 应用的数据瓶颈，通过标准化、智能化、合规化的数据全链路服务，将海量原始数据转化为可直接赋能大模型训练、RAG 智能检索、AI Agent 智能应用的高质量数据燃料，彻底解决企业 AI 落地的“数据就绪难题”。

针对行业普遍存在的数据孤岛、质量参差不齐、合规风险难控、工程落地断层、技术架构脱节五大核心难题，霍因科技打造行业领先的三段式全流程 AI 数据就绪解决方案，以完善的技术体系与知识体系，实现从数据合规梳理、数据精加工到 AI 智能应用落地的一站式闭环服务，全方位打通 AI 产业化落地的“最后一公里”。

3、创新赛道：全息网络事件定位与分析

领航者：兰云科技

全息网络事件定位与分析，兰云凭借搭载 Agent 智能体技术的 ai_soc 智能安全运营中心（CSP 5.1 底座），融合三大核心能力并共享数据底座，实现定位、溯源、

核验一体化。

一是网络故障自动精准定位，依托多源数据与拓扑推理，分钟级定位至网元及端口，快速给出排障方案；二是网络安全事件溯源，基于八阶段杀伤链，结合多项检测技术完整还原攻击链路，并完成 ATT&CK 战术映射；三是资产端口级精准定位，打通资产、端口与使用人关联，实现精细化隔离处置。

产品实现三大能力闭环联动，AI 判定过程可溯源核验，支持分层多版本报告，采用本地化大模型保障数据安全，异常状态可自动降级运行。该平台适配信创环境，已在政府、能源等关键领域落地，配套专属行为模型与威胁狩猎规则。整体大幅缩短故障与安全事件处置时长，降本增效，同时满足各类合规上报要求。

4、创新赛道：基于白环境的主机安全体系

领航者：联通数科

基于白环境的主机安全体系，核心逻辑是“换个思路，只做对的事”。不盲目去猜谁是坏人，而是通过技术手段，把主机中合法的资产、应用、进程和网络行为圈定为一个“白名单”。在这个环境里，非准许，即禁止。任何名单之外的未知程序或异动，都会被瞬间拦截，从根本上免疫未知威胁。

在联通云主机安全产品（“云堑”系列）中，这个理论得到了完美的实战工程化落地。

首先，采用了自适应安全架构。产品能够深度感知主机工作负载上的资产应用、运维操作和网络活动，自动生成安全指标。这就好比在主机内部建立了一个“全天候雷达”，持续分析、监控，自动识别出偏离“可信白基线”的异常行为，形成预测、防御、监控、响应的安全闭环。

其次，作为云原生安全产品，它最大的差异化优势在于“安全生于云、长于云”。

将可信白环境的构建，直接内生在租户的 VPC 内部。这意味着安全能力与云基础设施实现了同开通、同关停、同监控。

利用微隔离技术，把安全边界收缩到单个工作负载，精准抵御内网的横向渗透。客户不需要额外搭建复杂的资源池，在业务上线的同时，可信白环境就已经毫秒级就绪，既确保了等保与密评的合规，又实现了真正的高效降本。

5、创新赛道：暗网情报 DWI

领航者：零零信安

暗网情报 DWI，零零信安是国内领先的暗网威胁情报服务商，专注于为政府和企业提供全域暗网情报监测、数据泄漏检测及闭环事件响应服务。

依托跨协议蜘蛛爬虫、反爬对抗、高保真镜像及多模态 AI 模型，实时监测上万个暗网威胁源，已监测暗网情报 325 万，勒索事件 2.9 万，Telegram 消息 13 亿，泄露数据 216 亿。 监测范围覆盖上百个黑客论坛和暗网市场、数百个勒索组织及数千个 Telegram 群组，对外提供从情报监测分析到事件闭环处置的全链条应急响应服务。

零零信安已为政府、监管、金融、运营商、能源、制造、科技及互联网等上百家头部单位提供专业服务。

6、创新赛道：身份驱动的数据库安全

领航者：帕拉迪

身份驱动的数据库安全，帕拉迪专注于数据中心安全与智能领域，2005 年成立以来一直围绕身份访问安全和数据库安全两个细分赛道，以垂直专精为理念，深耕全球利基市场。

面向数据中心数据库的安全运维与防护，从数据库账号弱密码威胁，运维访问连接数据库人为操作的威胁，业务连接数据库业务流的攻击威胁等多个途径进行立体式

综合防御，从自然人关联、数据库攻防、数据滥用、安全审计等多维度，拥有流会话解析、网络反代等专利技术，具备高并发、高稳定、低时延、无感知、易接入等核心能力，提供了基于身份安全的数据库安全解决方案。

通过该方案，帮助客户实现数据库账号发现，账号密码集中存储、修改及分发，账号密码风险评估，让僵尸账号、幽灵账号一目了然。提供了统一的身份认证和安全管理界面，对开发人员、测试人员或第三方外包人员在数据库的安全接入、过程使用、数据库权限治理、运维动态脱敏等方面进行管控，做到数据库安全运维的事前预防、事中阻断和事后追溯。对于所有绕行的连接及访问进行阻断，业务行为白名单建模，防护针对业务系统的 SQL 注入攻击、0DAY 攻击、木马勒索、拖库等攻击行为。

7、创新赛道：AI 数据安全

领航者：闪捷信息

AI 数据安全，凭借在 AI 数据安全赛道的综合创新实力，入选“创新赛道领航者”。闪捷信息成立于 2015 年，深耕数据安全十年，拥有百余项国家发明专利，未来将持续以创新护航企业 AII 化转型，助力合规、安全释放 AI 价值。

技术能力上，闪捷信息秉持“AI 赋能安全，安全护航 AI”双轮驱动战略，自研 AI 数据智能引擎，在多模态数据智能识别、动态风险监测及自适应防护等方向实现突破。

产品创新上，闪捷信息在业界率先推出 AI 数据安全系列产品矩阵，构建覆盖智能体安全、AI 安全网关、内容风控、数据治理的产品体系，以“以智御智”为核心理念，帮助企业在 AI 应用浪潮中“看得见、管得住、流得动”。

目前，上述产品已广泛应用于客服对话、Agent 调用、RAG 知识库等场景，并在金融、制造、能源、通信等行业落地。

8、创新赛道：ASIC 专用芯片

领航者：山石网科

ASIC 专用芯片，山石网科的 ASIC 专用芯片通过工业和信息化部电子第五研究所的自主可控测评，符合国家相关标准，打破了国际厂商在高端安全芯片领域的长期垄断，实现了高端安全芯片核心技术的自主可控。通过“专用计算架构+芯片级卸载”技术路径，实现了五大核心性能的跨越式提升：

（1）算力性能突破性提升

吞吐性能实现约 3 倍提升，且保持大小包处理性能一致性，彻底解决传统架构在复杂流量场景下的性能衰减难题。同时，新建连接数提升约 2.5 倍，IPsec VPN 性能提升约 2 倍，突破传统设备的算力瓶颈

（2）超低时延保障实时业务

相较于传统防火墙数十微秒的时延水平，ASIC 防火墙可将时延稳定控制在≤4.8 微秒，降幅超 80%，完美适配实时交互业务场景

（3）高密度接口扩展能力

针对传统防火墙高速接口数量受限的痛点，ASIC 防火墙全系标配更多万兆接口，并支持 100G 高速扩展，为高带宽组网提供坚实基础。

（4）绿色节能低碳运行

通过芯片级卸载技术，整机功耗降低超 40%。显著提升能效比，契合国家“双碳”战略要求

（5）极致稳定可靠运行

与传统架构在高负载下 CPU 占用率飙升的情况不同，ASIC 芯片承担主要数据面负载，确保系统在高吞吐场景下仍保持低 CPU 占用率和稳定运行。

9、创新赛道：网络边界防御系统（NPS）

领航者：微步在线

网络边界防御系统（NPS，Networkperimeter Protection System），首创基于攻击视角，从出入站维度双向全面对网络威胁自动化防护。在网络边界防御中，创新研发四大核心防护技术能力——高精准情报主动防护、多维度封禁自动防护、0day漏洞精准防护、灵活开放的第三方联动封禁，重新定义了边界防御新范式。

微步威胁防御系统 OneSIG 是专为网络边界打造的高性能安全防御网关，以基于精准检测的自动化封禁为特色，融合高精度情报实现出入站威胁的实时发现与自动化拦截，有效过滤恶意流量，打造现代安全运营第一防线。

相较 IPS 的核心优势： 传统 IPS 仅做入侵威胁检测，不做失陷反连威胁检测；依赖特征规则匹配，对 0day、黑产变种等新型攻击检不出；误报率高导致大量规则仅监控不拦截；IP 封禁容量有限，海量黑名单迅速触及性能瓶颈；缺乏加密流量检测能力；联动封禁依赖人工操作，响应滞后。

OneSIG 凭借情报驱动的精准检测替代规则堆叠，用自动化封禁替代手动研判，用千万级封禁性能替代有限黑名单，用 0day 主动防护替代被动等补丁，既检测入侵威胁，也检测失陷反连，实现了从“能看见”到“能拦住”再到“自动拦”的根本性跨越。这是传统 IPS 仅靠规则匹配、手动配置拦截所无法企及的。

10、创新赛道：大模型赋能全链路合规测评

领航者：有略人工智能科技（北京）有限公司

大模型赋能全链路合规测评，北京有略人工智能科技深耕合规测评赛道，依托人工智能大模型打造全链路智能化测评能力，聚焦网络安全等级保护、商用密码、关键信息基础设施、数据合规及个人信息保护五大领域，自主研发全套 AI 智能合规测评

工具系统。

产品赋能三类主体：

- 面向测评机构：依托有略 速鉴、密鉴等 AI 测评工具系统，高效解决测评效率低、流程不规范、报告质量差等痛点，从技术层面杜绝假测、漏测、敷衍测评的乱象；
- 面向直接用户：依托有略慧鉴 合规管理运营系统，实现历年来测评报告可视化数字管理、风险归集与整改任务闭环追踪；
- 面向监管单位：依托有略质衡 AI 审核工具系统，实现测评过程与结果智能化审核管控。

有略全系列产品，严格对标国家法律法规、国家标准及现行监管规范，确保测评过程真实合规、测评结果精准可靠。

第五章 数字安全·资本

自数世咨询提出“科创无望，北交拥堵，港交在望”的观点之后，已有五家安全企业先后在港交所提交申请。在科创板改制落地之前，国资收购逻辑基本不通的情况下，港交所可能是资本仅有的退出路径。

—— 数世咨询

第五章 数字安全·资本

数世咨询统计，2025 年国内数字安全企业股权融资仅为 20 笔，相比于 2024 年大幅下降 62%。股权融资总额仅约 6 亿元，与 2024 年（25 亿元）相比大幅下滑 76%。收并购数量基本持平，有 8 起，平均并购金额 6000 万元左右。

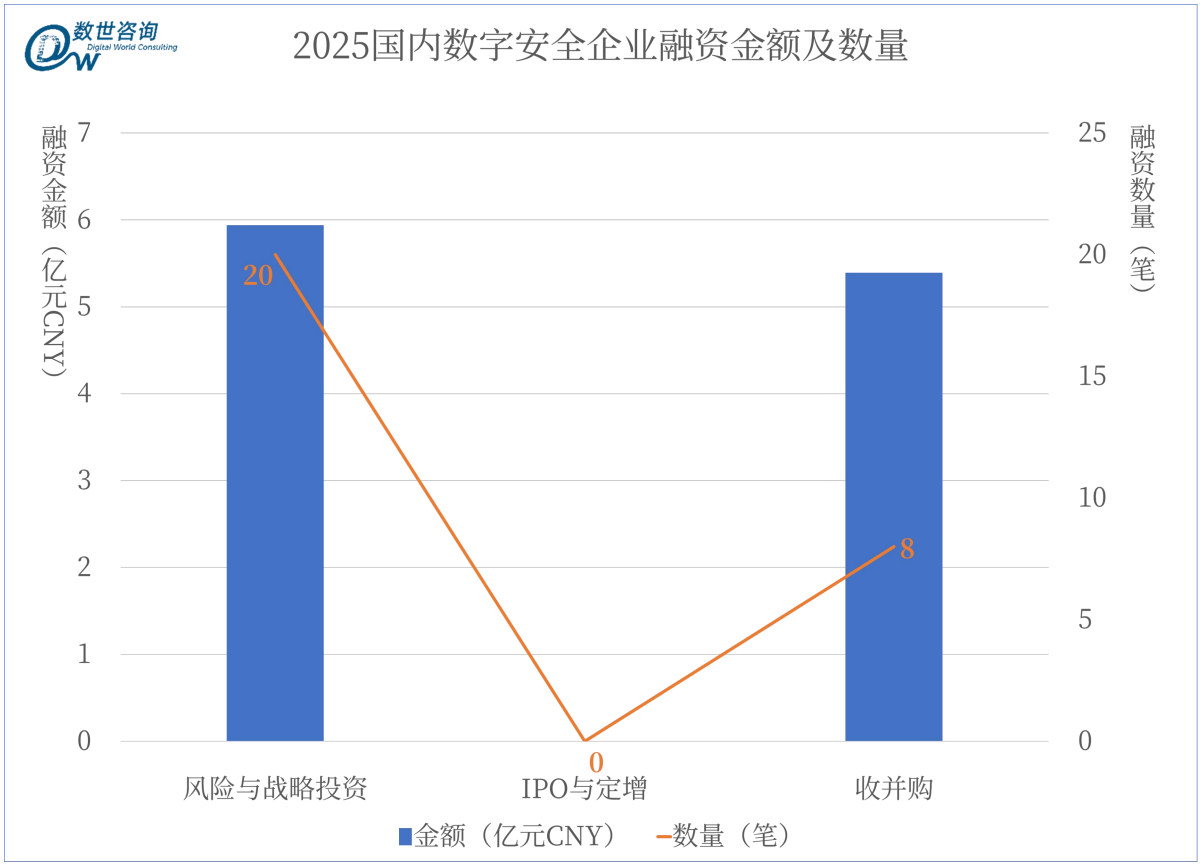


图 5-1 数字安全企业融资概况（2025）

图 5-2 2017-2025 年国内数字安全资本市场概况

- **重要结论**

❖ 自 2021 年近 170 亿元融资总额的历史最高点出现后，开始连续断崖式下跌。2022 年 100 亿，2023 年 39 亿元，2024 年 25 亿，2025 年 6 亿。

❖ 民间资本几近停滞，国有资本极度谨慎。后者在并购时，提出不能亏损、PE 估值、亿级规模和业绩对赌的四项基本原则。而当下的经济环境，很难有企业满足所有这四项条件，而真正符合这些条件的企业则根本没有并购意愿。

结　语

2025 年，中国国民生产总值为 140.19 万亿元，本报告统计的数字安全市场规模为 887 亿元。美国国民生产总值为 30.77 万亿美元，数字安全市场规模约 850 亿美元。也就是说，中国的数字安全市场规模仅为 GDP 的万分之 6.3，而美国的比例是千分之 2.8，两者相差四倍。

安全天然具有公共属性，因此东西方各国的监管机构都会高度重视。无论是消防安全、交通安全、生产安全，还是公共安全、社会安全、国防安全，各个领域的安全产业都是强合规驱动的。数字安全产业也不例外。但为什么同样是强合规驱动，中国的却走向了纸面合规或形式合规的道路?

笔者认为，惩罚力度与数字化依赖程度，是最为关键的两个因素。前者是外因约束，后者是内因驱动。

首先是外因。许多人都听说过“严格立法、选择执法、普遍违法”，正是因为违规成本过低，导致违规比守规更划算。而“运动式”与“脉冲式”的检查进一步固化了纸面合规的生存空间。然后是内因。业务与安全脱节，很多国有机构的数字化转型停留在 OA 办公、档案管理、官网展示、通报上报等浅层信息化应用，核心业务依然在线下，安全自然属于边缘化的成本中心。

其实，中国数字安全产业的痛点、难点、卡点、堵点还有很多，远非这一本报告所能阐述与承载。“道阻且长，行则将至”，作为第三方独立调研机构，数世咨询将一如既往，持续为业界提供客观翔实的数据，专业的观点和深刻的洞察。

—— 数世咨询 2026 年 6 月

附录：统计标准

“一套清晰明确并来源于实践的统计标准，其意义甚至要大于统计工作本身。因为没有统计标准，统计工作就是空中楼阁。”

—— 数世咨询 2022.6

本报告的统计标准包括，统计口径、统计范围、调查方法和术语解释，供业界相关人员参考与指正。

一、统计口径

本报告的统计口径有两大类，一类是公开财报的上市企业，以**财报披露**的营收额为准。另一类是未上市的公司，以年度的营收**开票额**为准。

本报告包括三种整体市场规模的统计数字，即数字安全行业总收入、数字安全业务（含集成）总收入和数字安全业务（去集成）总收入。如无特别指出，本报告所提及的数字安全市场规模是指“**数字安全业务（含集成）总收入**”。

统计数据的时间跨度为 2025 年 1 月 1 日至 2025 年 12 月 31 日。

二、统计范围

基于数世咨询核心团队 20 年的国内安全企业调研工作的经验积累，本报告根据原厂能力、营收水平和业务类型，选择了 800 余家在公开市场上具有一定知名度的数字安全企业作为本报告的基础调查对象。

- 本报告的统计范围为中国内地的企业，不包括香港、澳门和中国台湾地区。
- 本报告的基础调查对象为 800 余家经营数字安全业务且具备原厂能力的企业，**不包括**专门从事分销、代理、代售业务的企业，和不具备解决方案能力的集成商，以及非企业主体，如研究所、测评中心、高校学院等。
- 在 800 家基础调查对象中，本报告以 1000 万元左右的数字安全业务年营收额为底线，选取了 400 余家企业作为统计对象。
- 信创领域中，如芯片、操作系统、数据库、中间件、服务器、个人电脑、办公软件等非安全类产品不在本报告统计之内。

三、统计方法

- 在调研方面，本报告主要通过企业问卷调查、公开资料收集、**日常交流访谈**三种形式开展调研工作。
- 在统计方面，本报告采用的是**供给侧的角度**，将统计对象，即 400 余家数字安全企业的年营业收入、业务类型、从业人员、地区行业收入等数字进行计算后，从各种不同的维度进行展现。
- 在收入方面，**数字安全业务收入**在企业总收入中占比小于 50%的企业，只统计数字安全业务收入，不统计该企业的非安全业务收入。反之，占比大于等于 50%的企业，则需要统计其非安全业务，并将其与安全业务共同计入**数字安全行业收**入。
- 在收入划分方面，弃用软件与硬件收入的划分方法，将两者合而为一并且与“软件即服务”收入一并计入**安全产品收入**。

四、术语解释

1. 数字安全：数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展的政策法规、管理措施、技术方法等安全手段的总和。

2. 数字安全业务：以企业主体出售网络安全和数据安全产品、人员服务、解决方案产生的经营收入。

3. 数字安全企业：理论上一切具有数字安全业务的企业都可称之为数字安全企业，但在本报告的统计对象中只包含了数字安全业务占企业总收入 50%及以上，或者数字安全业务年收入达 1000 万元以上，且具备原厂能力的企业。

4. 原厂能力：自身具备数字安全产品研发、方案定制、安全服务的能力，而非单纯的中间转售。

5. 数字安全企业从业人员：与数字安全企业签订劳动合同的正式员工。

6. 数字安全技术或网络安全技术：本报告中一般是指数字安全企业所提供的产品、服务、方案的其中一种、两种或总和。

北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业800余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接、安全产品与企业推荐、企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www. dwcon. cn
联系邮箱：dw@dwcon. cn

数世咨询
Digital World Consulting

国内数字化领域独立第三方调研咨询机构