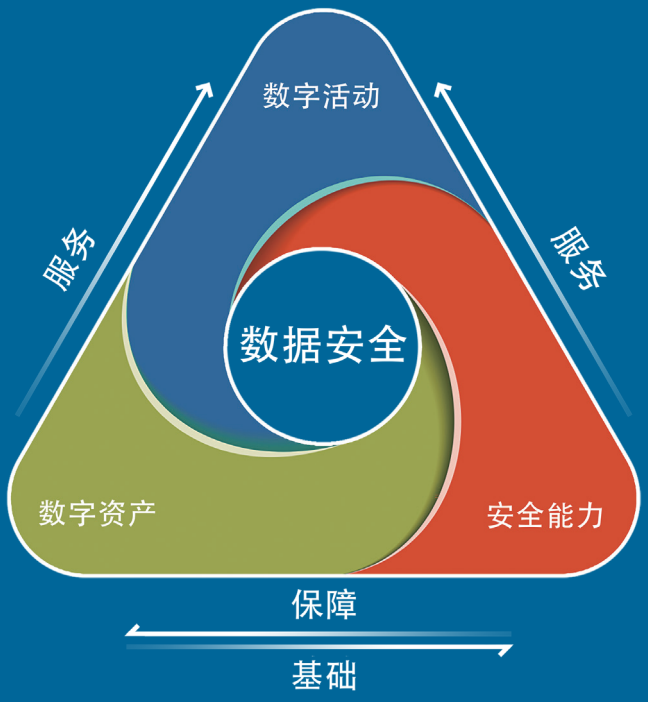
数世咨询
Digital World Consulting

中国数字安全产业年度报告 (2023)

数世咨询
Digital World Consulting

中国数字安全产业年度报告 (2023)



数字世界　以网络连接为基础，以数据流动释放价值，以人工智能塑造未来。
数字安全　以网络安全为基本手段，以数据安全为核心目的，支撑数字经济的健康发展和国家社会的和谐稳定。
数字世界，安全共生！

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构、企业用户等合作伙伴提供数字安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

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　**左　晶**
统计分析师　**牛爱民**
数世智库　数字安全能力研究院

版权声明

目　录

目 录

目　录

前 言

2020 年至 2022 年，是全球动荡变化的三年，战争、疫情、贸易封锁、金融危机……习总书记近年来数十次的强调“当今世界正经历百年未有之大变局”。具体到仅有三十年历程的网络安全产业，如今也面临着前所未有的挑战和机遇。

三年疫情之后，广大安全企业面临着生存与发展，创新与营利的多重难题。但危机与机遇并存，数字化的趋势已是全球共识，数字经济已是所有经济体的发展目标。因此，网络安全正在从以国家安全、公共安全为主的范式转换到国家安全保障和护航数字经济并重的数字安全。数字经济的命脉是数据的流动，因此，以网络安全为基础手段，以数据安全为核心目的，是数字安全的技术内涵。

在万物互联的数字世界里，数字安全是国家安全和数字经济的基础支撑，而摸清家底、厘清现状，以判断趋势和辅助决策，是助推数字安全产业健康良性发展的前提。为此，数世咨询基于连续多年积累的产业调研能力和经验，经过大量的现场沟通、访谈，梳理、整理，统计工作之后，撰写完成《中国数字安全产业年度报告 (2023)》，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

2023 年 6 月

第一章　统计标准

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

——摘自《中国数字安全产业统计与分析报告（2022）》

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，本报告所有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 2022 年 1 月 1 日至 2022 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 750 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、澳门和台湾地区内。

●本报告的基础调查对象为 750 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，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 750 家基础样本中，本报告以 1000 万元左右的数字安全业务年营收额为底限，选取了 350 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 350 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，则统计其非安全业务并将其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”收入一并计入到安全产品收入。

四、术语解释

1、数字安全

包含电子设备、通信网络、信息系统及电子数据所构成的虚拟网络空间，正在与现实物理空间融合成一个数字化的世界。在数字世界中，面向数字化对象或基于数字化手段而展开的对抗博弈过程，称之为数字安全。

2、数字安全业务

以企业主体出售数字安全产品、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，但在本报告中是指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、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。

7、并购

兼并和收购。本报告中是指并购双方或多方相互之间的股权转移，而不是以融资为目的的股份稀释。

（注：本章的统计标准部分参考中国网络空间安全协会于 2020 年发布的《中国网络安全产业统计报告》。）

第二章　数字安全·市场

网络安全行业发展了三十年，从计算机安全等级保护，到信息安全等级保护，再到网络安全等级保护，充分体现出合规的第一驱动作用。但数字安全的复杂性和碎片性，只能依靠创新来引领和解决。数字安全行业的未来，一定是合规与创新双轮驱动。

——摘自《2022 年数字安全大事记》

一、市场规模

2022 年度，国内数字安全业务（含集成）总收入为 981.2 亿元，较 2021 年度增长 7.14%。与上年度 18.6% 的增长率相比，下降 11.46 个百分点。数字安全集成业务收入 199.72 亿元，较 2021 年度增长 36.42%。

2022 年度，国内数字安全业务（去集成）总收入为 781.48 亿元，较 2021 年度下降 14.92 亿元，增长率为 -1.87%。与上年度 15.9% 的增长率相比，下降 17.77 个百分点。

2022 年度，国内数字安全行业总收入为 1047.81 亿元，较 2021 年度增长 6.97%。与上年度 22% 的增长率相比，下降 15.03 个百分点。

（注：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）

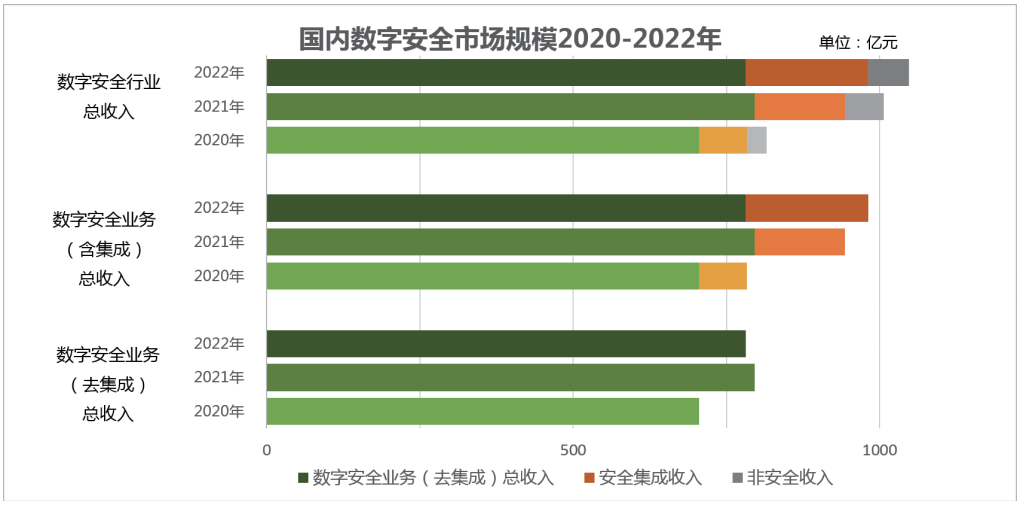


图 1　国内数字安全市场规模 (2020-2022)

新冠疫情三年（2020-2022）期间，国内数字安全产业规模的变化为“先扬后抑”。从 2020 年增长率 29.9% 的历史最高点，下滑到 2021 年的 18.6%，然后再到 2022 年的 7.14%，成为 2014 年以来的历史增长率最低点。这一结果，基本符合数世咨询去年报告中的市场预判。

“2022 年度的数字安全市场有可能出现自 2014 年以来的历史最低增长”—摘自《中国数字安全产业统计与分析报告 2022》

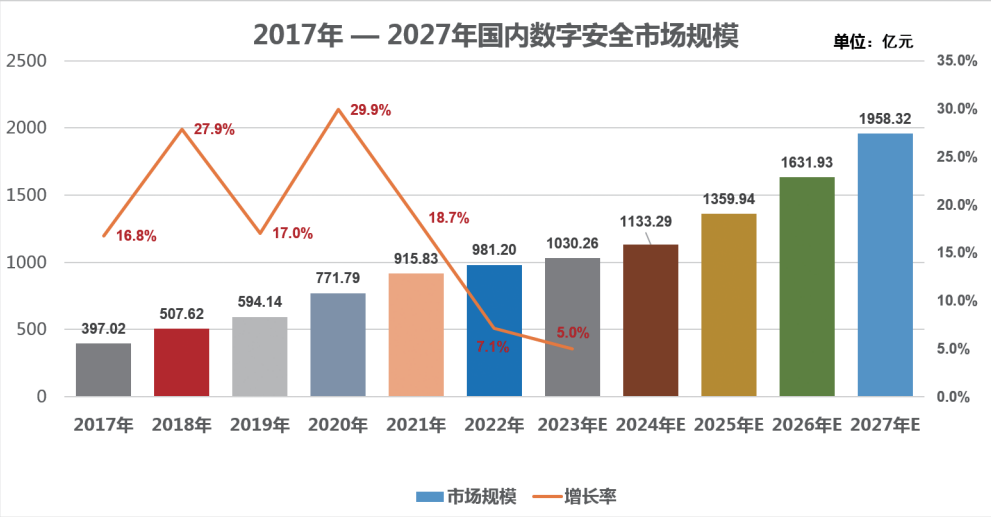


图 2　2017-2027 年国内数字安全市场规模

重要结论

●2022 年度，国内数字安全市场规模为 981.2 亿元，增长率首次跌破两位数，仅为 7.14%，为十年来的历史最低点。

●需要业界尤为警惕的是，7.14% 的市场规模增长，实际上完全来自于集成业务，而安全产品和服务则首次出现负增长即 -1.87%。

●在全球经济疲软的大背景下，以 2022 年底数字安全需求方的预算规划和今年上半年预算的实际执行情况来看，2023 年的市场形势十分严峻，大概率继续维持个位数的增长率。

●以 2025 年，即十四五规划收关年，恢复 20% 的增长率推算，国内数字安全市场规模将在 2027 年接近 2000 亿元。

二、业务分类

正如去年报告所言，将数字安全产品划分为硬件和软件的习惯，来源于生搬硬套传统信息产业的划分方法，不适用于以生产软件和提供服务为主的数字安全厂商。依据数世咨询的统计惯例，本报告将数字安全业务分为三大类：一是软硬件、设备及 SaaS 订阅收入，即安全产品收入；二是以人天计费的安全服务收入；三是安全集成收入。

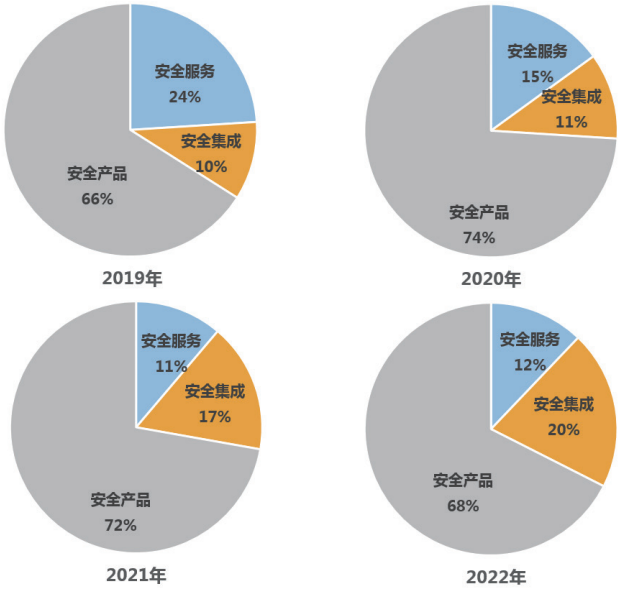


图 3　2019-2022 年 安全产品、安全服务、安全集成占比

重要结论

●2022 年，安全产品收入约占总收入的 68%，安全服务收入约占总收入的 12%，安全集成收入约占总收入的 20%。

●安全服务占比略有上升，安全产品占比下降，安全集成业务连续三年呈快速上升态势。

●安全集成业务占比的提升，有两大主因：

一是多元化。大型安全企业、云服务商和软硬件科技企业均不同程度的在

发展集成业务，以扩大营收规模。

二是数科化。大型国有集团纷纷成立科技三产公司，或改组或合并原有组织架构，以获取更大的竞争优势。

三、客户分布

根据本报告 750 家基础调查对象客户数据的不完全统计，2022 年数字安全产业的核心客户群依然为，政府部委、国防公安、金融、运营商和能源等五大领域。

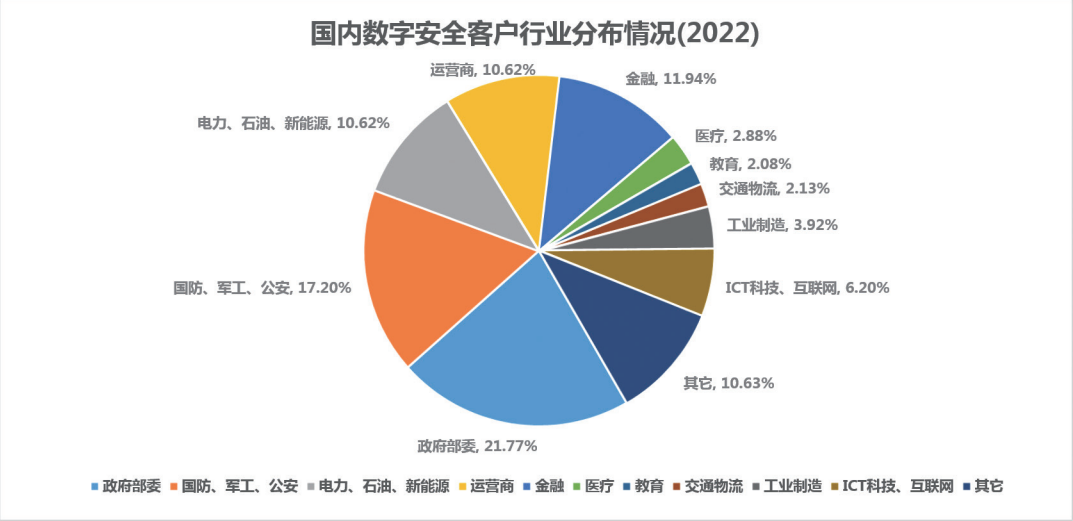


图 4　国内数字安全客户行业分布情况 (2022)

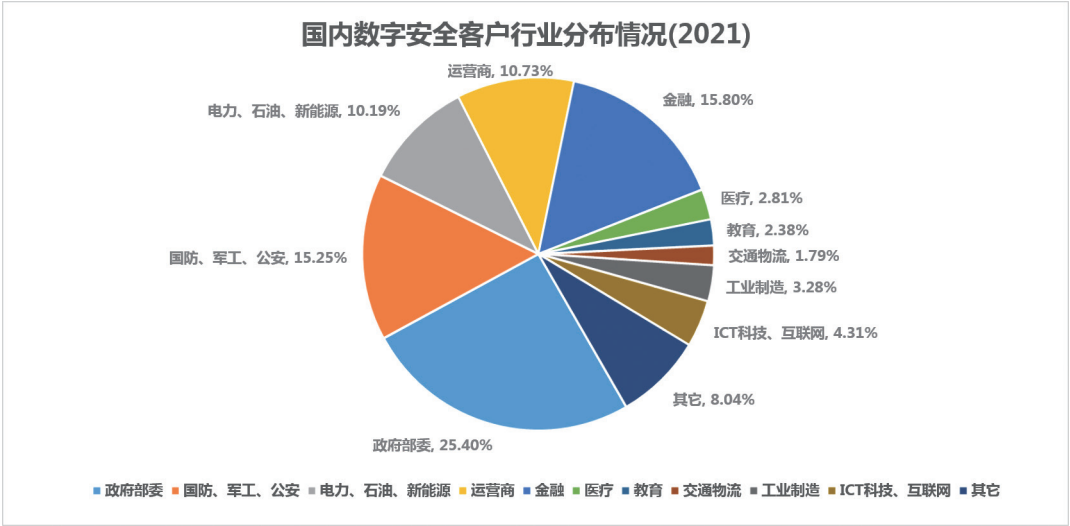


图 5 国内数字安全客户行业分布情况 (2021)

重要结论

●疫情原因，政府部委（不含国防、公安）在客户行业中的占比明显下降，但国家与社会安全等特殊行业，以及事关国计民生的工业制造、医疗、ICT 科技和互联网领域等领域，占比均略有上升。

●由于安全具有国家、社会、政治等公共属性，因此合规始终是数字安全产业的基本驱动力。但随着全球的数字化进程，数字经济发展带来的应用场景需求将会成为数字安全的第二大驱动力。

四、城市分布

按数字安全企业总部所在城市的企业营收排序，超过 20 亿元的有九座城市，分别为北京、深圳、杭州、成都、上海、南京、厦门、苏州、济南。从各城市数字安全企业收入占城市 GDP 的比例来看，除北京、深圳和杭州三所城市以外，其他六座城市均有很大的提升空间，尤其以上海为甚。

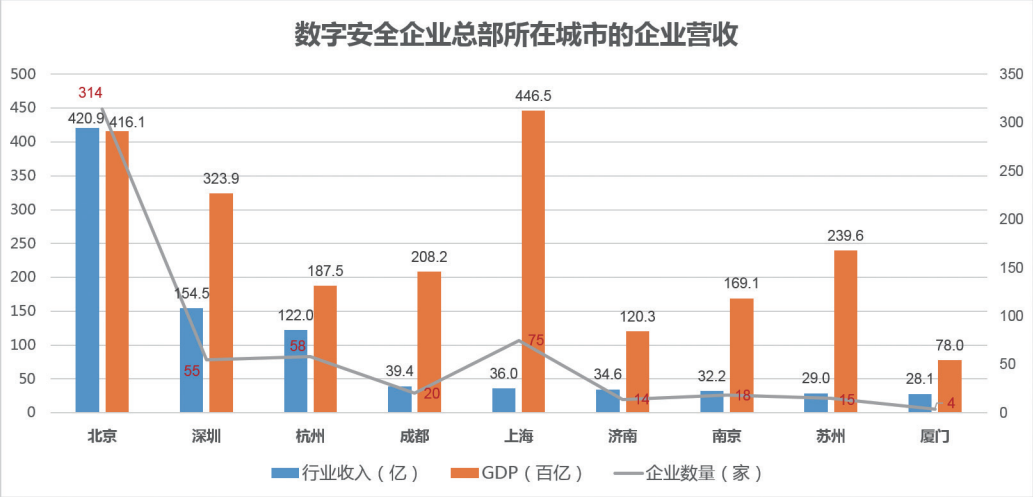


图 6　数字安全企业总部所在城市的企业营收

第三章　数字安全·企业

从各企业收入水平的占比情况来看，网络安全市场“没有寡头，只有诸侯”的格局明显，同时碎片化现象非常突出。这种情况也与全球网络安全市场的格局相似。

——摘自《2020 年中国网络安全产业统计报告》

一、收入水平

2022 年的数字安全业务（含集成）年收入，在本报告 350 家统计对象中，有 11 家企业收入达到 20 亿元以上，占比 37.5%；8 家达到 10 亿元以上，占比 12.6%；18 家企业在 5 至 10 亿之间，占比 12.9%；133 家企业在 1 至 5 亿之间，占比 29.6%；180 家企业不足亿元，占比 7.1%。

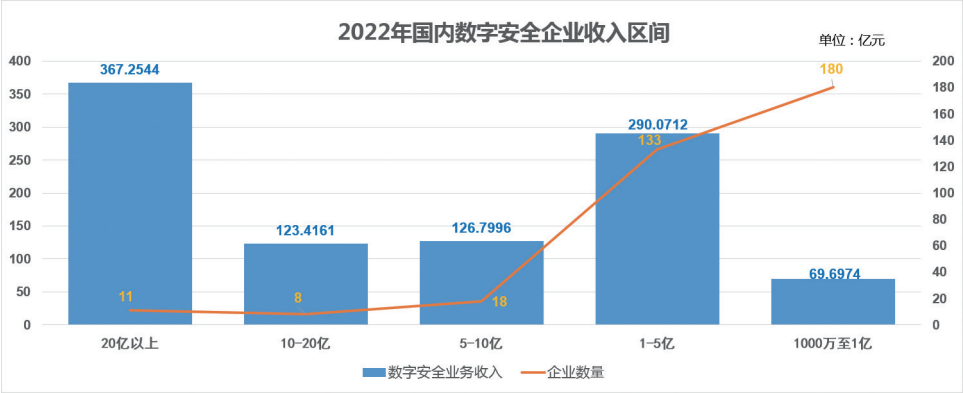


图 7　2022 年国内数字安全企业收入区间

重要结论

●与去年相比，数字安全企业的年收入水平几无变化。数字安全技术属于企业服务的市场范畴，碎片化的格局是常态。“没有寡头，只有诸侯“的市场格局，未来将长期保持下去。

●对于数字安全企业而言，一方面很难快速的规模化，上市的比例很小。另一方面能保持基本的企业运转，破产倒闭的情况很少。因此，在扎根自身的特长领域和保持创新力的基础上，实现良性循环、稳步增长的目标，不失为中小企业的健康经营之道。

二、上市企业

2022 年度，具有明显数字安全业务属性的企业，在新三板挂牌的公司有

38 家，在沪深上市的共有 51 家。其中，数字安全企业 32 家（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）。

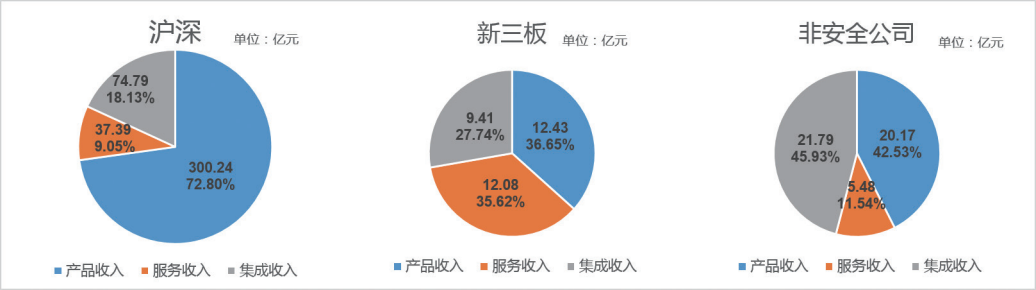


图 8　具有明显数字安全业务属性的上市企业收入分类

另据今年 5 月数世咨询发布的《2022 中国数字安全上市企业航线图》的统计，自数世咨询 2014 年开始产业统计工作以来，沪深上市的数字安全企业净利润总和历史上首次出现亏损，且亏损总额接近 17 亿元。

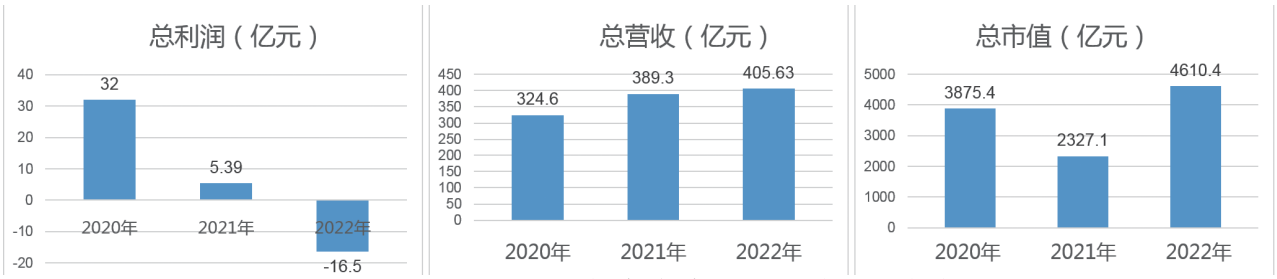


图 9　2020-2022 年数字安全上市企业三项指标

重要结论

●从上市企业收入分类中可以明显看出，沪深两市的企业以产品销售为主，而新三板企业服务与集成并重，而仅有安全业务属性的非安全公司，则是集成和产品并重。

●净利润历史上首次出现亏损，具体表现在 25 家企业出现亏损，更甚者一家企业高达 18 亿元的净利润亏损，即将出现历史上首个从沪深交易所退市的安全公司。

●在营收几无增长且亏损总额接近 17 亿元的情况下，但研发投入依旧有较高增长，除了部分有平衡财务指标的原因以外，还意味着安全上市企业对未来

的市场较有信心。

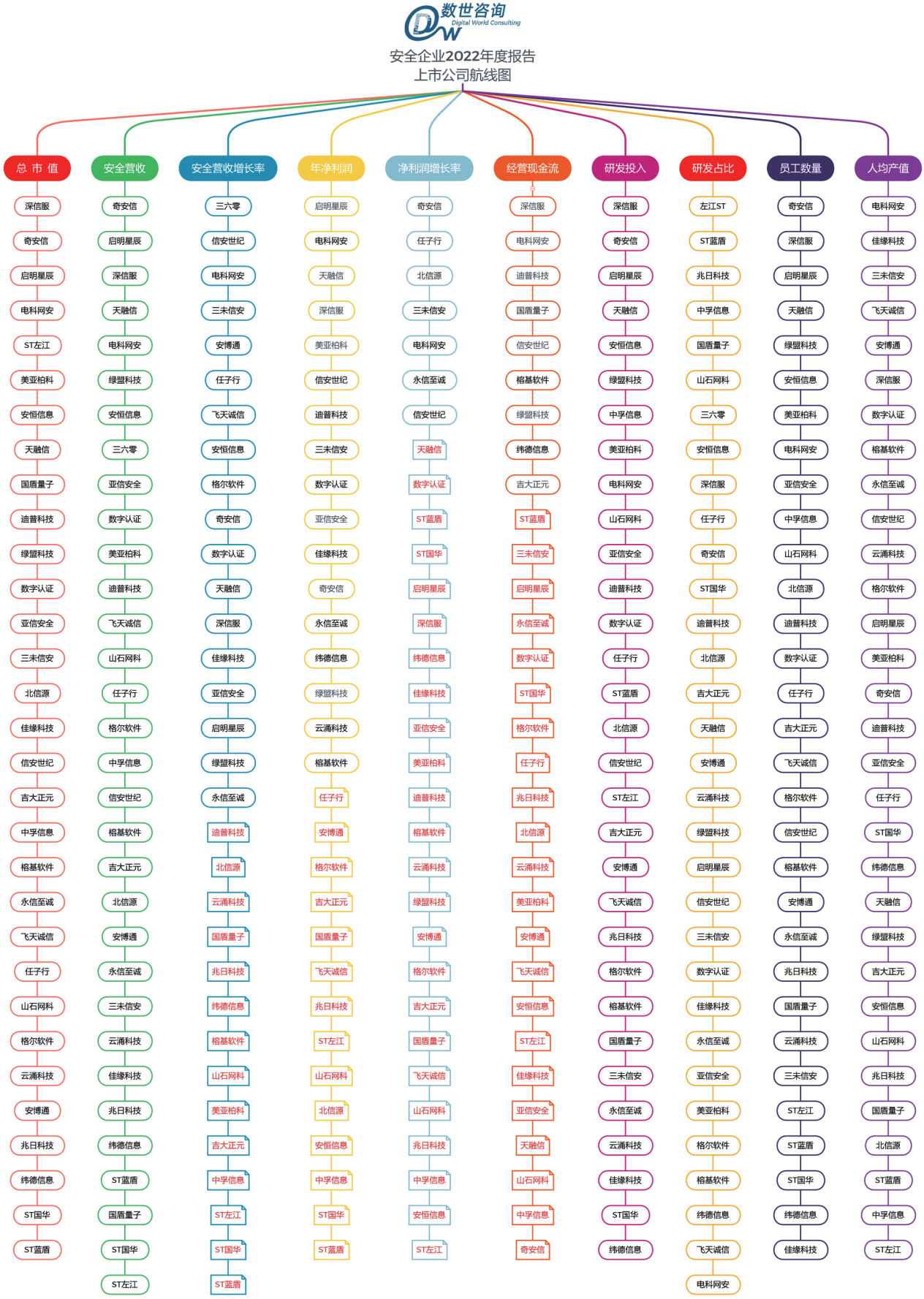


图 10　2022 中国数字安全上市企业航线图

三、数字安全百强

数字安全百强报告基于国内750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。报告分为两大部分，一是综合实力较为突出的100家企业，通过品牌影响力和企业规模二大维度，以数轴点阵图的形式予以展现。二是专精特新100家企业的推荐，目的在于突出业务规模目前较小，但在创新能力方面表现优秀的企业。

1、综合实力百强

在入围本次综合实力百强的企业中，领军力量企业入围门槛为10亿元，共19家，总营收约480.67亿元。中坚力量共45家，总营收约为220.71亿元。潜在力量共36家，总营收约为68.02亿元。

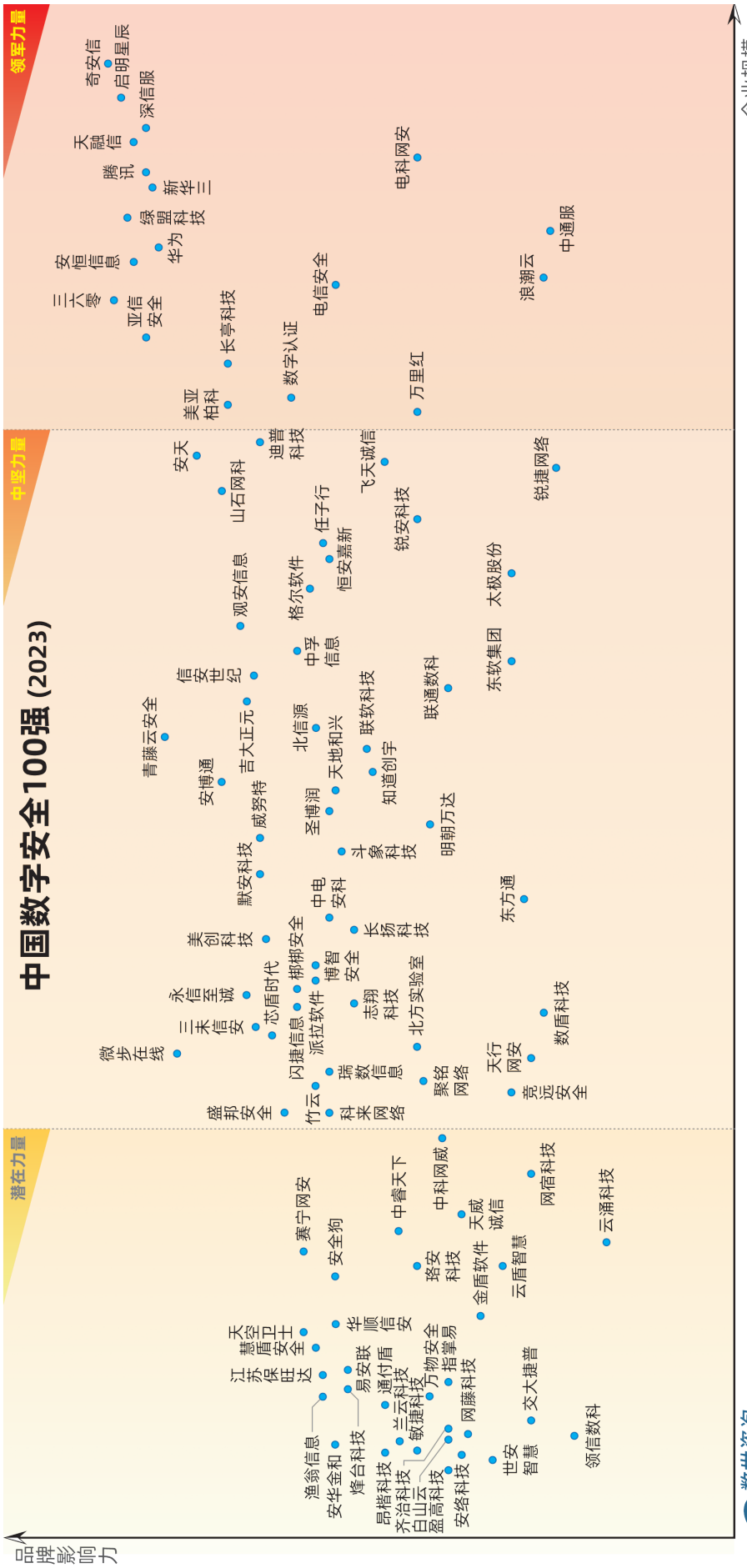


图 11　2023 年数字安全百强

2、年度成长力十强

即便在整体安全产业增长乏力的情况下，仍然有一批企业业绩突出，增长迅速：

图 12　年度成长力十强

3、年度创新力十强

创新是产业良性发展的灵魂支柱，在尤为注重技术实用性和应用价值性的数字安全领域更是如此：

图 13　年度创新力十强

4、专精特新百强

专精特新百强均为企业规模较小，但在专业、深度、差异化和创新性方面非常具有优势或特色的数字安全企业。由于名单较长，本报告仅列出“年度创新力十强”企业。（百强报告可前往数世咨询官网或公众号查看）

重要结论

●2022 年度，综合实力百强安全业务总营收达 769.4 亿元，较上年度增长 4.07%。年增长率下降约 12 个百分点。

●在本统计年度的综合实力百强中，有 5 家企业退出 10 亿元营收的领军力量区间，但也有 2 家企业首次挺进。

●专精特新百强中，开发与应用安全、威胁检测与响应、工业互联网安全、安全运营、数据安全、API 安全、数字靶场，为七大热点赛道。

●百强报告中，10 亿元区域企业数量的减少，意味着数字安全企业扩大规模的艰难。具备经营状况良好、规模大，并且创新力强的“三合一”型数字安全企业，在国内始终未能出现。

●数字安全产业的本质是企业级服务，只要是普及性的服务就一定是碎片化的。因此数世咨询认为，在自身擅长的领域深耕，合理调配现有资源，以实现“滚雪球”式的稳健增长，才是企业级服务市场的正道。

四、从业人员

2022 年数字安全企业从业人员约 14.71 万人，其中技术人员约占 69.7%，从业人员较 2021 年增长 6.6%。

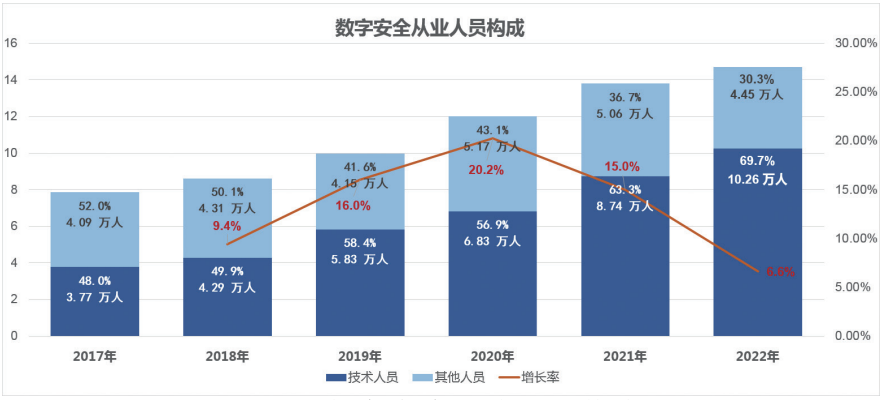


图 14　数字安全从业人员构成

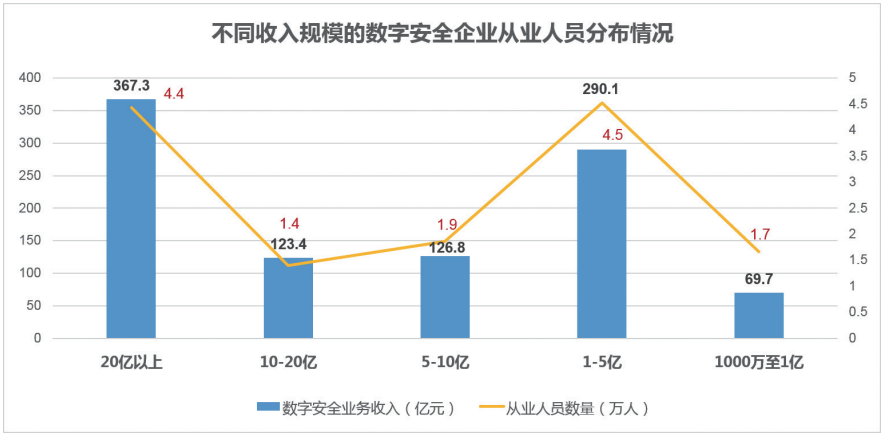


图 15　不同收入规模的数字安全企业从业人员分布

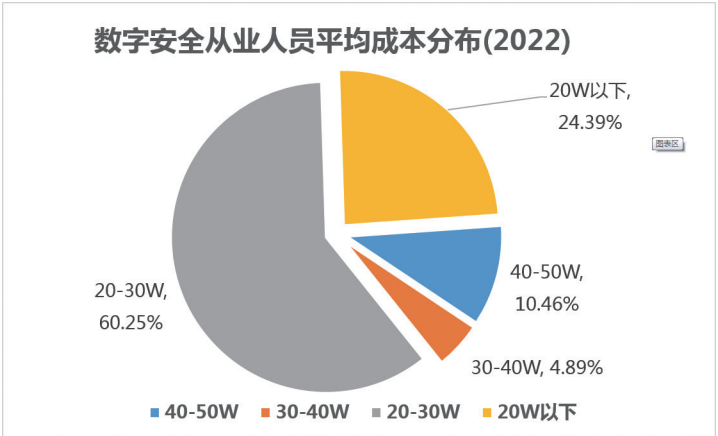


图 16　数字安全从业人员平均成本分布（2022）

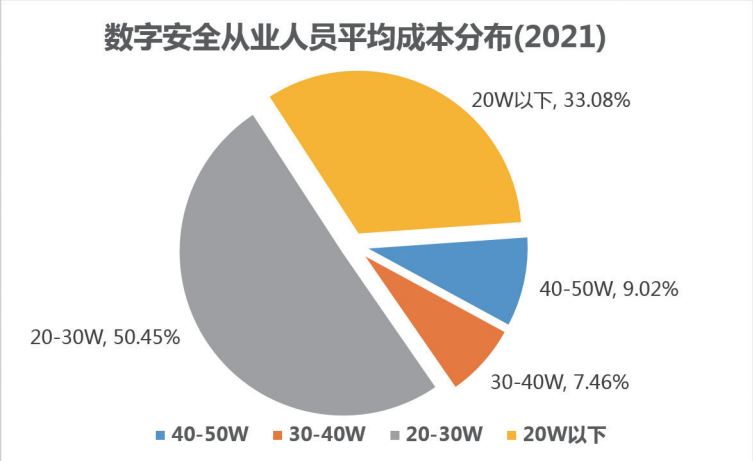


图 17　数字安全从业人员平均成本分布（2021）

重要结论

●2022 年，从业人员增长率为 6.6%，相比去年下降 9 个百分点，主要为非技术人员的减员。

●2022 年，数字安全从业人员的人均产值约为 53.86 万元，但人均净利润为负值。因此预计，2023 年整个产业的研发投入将有大幅度的缩减。

●2022 年，数字安全从业人员人均成本在 20-30 万元之间的占 60%，人均薪酬在 20 万元以下的占 24%。与 2021 年相比，前者增长了 10 个百分点，后者则下降了 10 个百分点。可以看出，数字安全从业人员成本（薪资水平）明显上升。

第四章　数字安全 • 技术

网络安全与数字安全最大的区别在于，前者的关注重点在“围绕通信、边界和端点组成的网络进行对抗的过程”，后者则是“**以网络安全为基础手段，以数据安全为核心目的。**”

——数世咨询

一、数字安全的内涵

自 2019 年数世咨询创始人在公开发表的文章中，首次提倡“数字安全”时代以来，数字安全的概念越来越受到业内的关注。

基于网络安全的本质和特性，数世咨询在 2020 年提出网络安全技术分类的方法论—“网络安全三元论”（以下简称三元论）：信息技术、业务应用和网络攻防。

信息技术是网络安全的起源。有了电子通信才有电子对抗，有了计算机、操作系统、数据库、应用程序，才会有系统安全、数据库安全、应用安全，有了云计算、移动互联网、工业互联网，才会有云安全、移动安全和工业互联网安全的概念。简而言之，没有网络就没有网络安全。

业务应用是一个机构或组织生存发展的根本前提，信息技术是为业务需求服务的。基于产品设备或技术方案对信息系统的保护，并非网络安全的最终目的，只有更好的服务数字化业务的需求，为数字经济的发展赋能，保卫国家安全，才是网络安全的根本目标。

网络攻防的逻辑本质是“对抗”，对抗则意味着没有无往不胜的攻击，也没有牢不可破的防御。“道高一尺，魔高一丈”，循环往复，永不休止。因此，动态性、相对性、整体性、开放性、协同性等理念是做好网络安全的方向指引。

2020 年，《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》）正式公布。《意见》开创性地把数据与土地、劳动力、资本、技术并列，定义为人类经济活动的第五大生产要素。2021 年，《数据安全法》实施。

2022 年，中共中央、国务院印发了《数字中国建设整体布局规划》，明确要求“筑牢可信可控的数字安全屏障。切实维护网络安全，完善网络安全法

律法规和政策体系。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。”

基于三元论的三大支点——信息技术、业务应用和网络攻防，围绕数据的安全保护，就构成了数字安全模型。网络安全与数字安全最大的区别在于，前者的关注重点在“围绕通信、边界和端点组成的网络进行对抗的过程”，后者则是“以网络安全为基础手段，以数据安全为核心目的”。

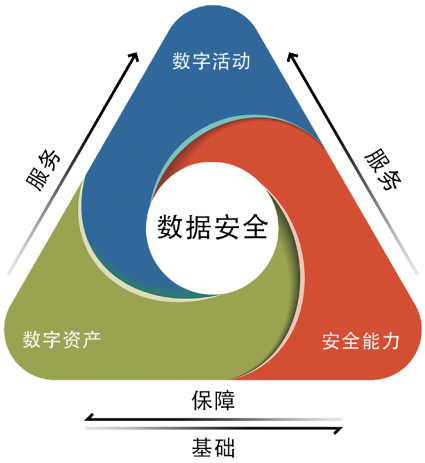


图 18　以三元论为支点的数字安全模型

重要结论

●信息技术是网络安全的保护对象，业务应用是网络安全的服务对象，而网络攻防是网络安全的立身之本。对三者的深度理解和技能掌握是做好网络安全工作的三个支点，缺一不可。数世咨询将这一理论称之为，网络安全三元论。

●以网络安全三元论为支点，数世咨询给出数字安全的概念：“包含电子设备、通信网络、信息系统及电子数据所构成的虚拟网络空间，正在与现实物理空间融合成一个数字化的世界。在数字世界中，面向数字化对象或基于数字化手段而展开的对抗博弈过程，称之为数字安全。”

二、数字安全能力图谱

从信息技术、业务应用与网络攻防三大支点和位于中心的数据安全共四大维度出发，能力图谱划分出八大方向，信息基础设施保护、信息计算环境保护；行业环境安全、应用场景安全；基础与通用技术、体系框架、安全运营；数据安全。每个方向又包含各自一级或子级的细分领域。（注：包含企业的完整版图谱可在数据咨询官网 www.dwcon.cn 浏览）

业内有很多缺乏逻辑框架，仅靠罗列堆积的企业目录、产品大全性质的图表，“重数量轻质量”、“只堆积不精选”、“模仿意愿强、原创能力弱”，是这些分类图表的普遍现象。常见的典型例子，一家年收入仅数千万元的厂商，就能覆盖十余个分类，一些综合产品的大厂更是能覆盖几十个分类。稍微有几年安全行业经验的人应该都明白，哪怕是一项细分品类的安全技术，都需要包括研发、人员、销售、市场、客户等方面的长期投入，一个数千万年收入的厂商能有二、三款主打产品已是极限。因此，一个貌似大而全但在真实性方面欠缺的图表，给业界带来了沟通不便、统计不便、采购不便等一系列弊端，违背了分类图谱清晰划分并推荐优选的初衷和本意，即降低供需双方的试错成本。

为此，数世咨询发布的系列能力图谱，大幅度削减了入选企业的数量，是精选而不是海选，更不是企业大全，以规避“全能型”原厂商或中小企业占据多条产品线的混乱现象。除此之外，为了反映重要行业用户中的主流安全厂商，数世咨询基于行业的维度，于 2023 年 6 月首次推出了《2022 年度中国数字安全能力图谱（行业版）》，包括了数字安全产业十个最为重要的行业领域。

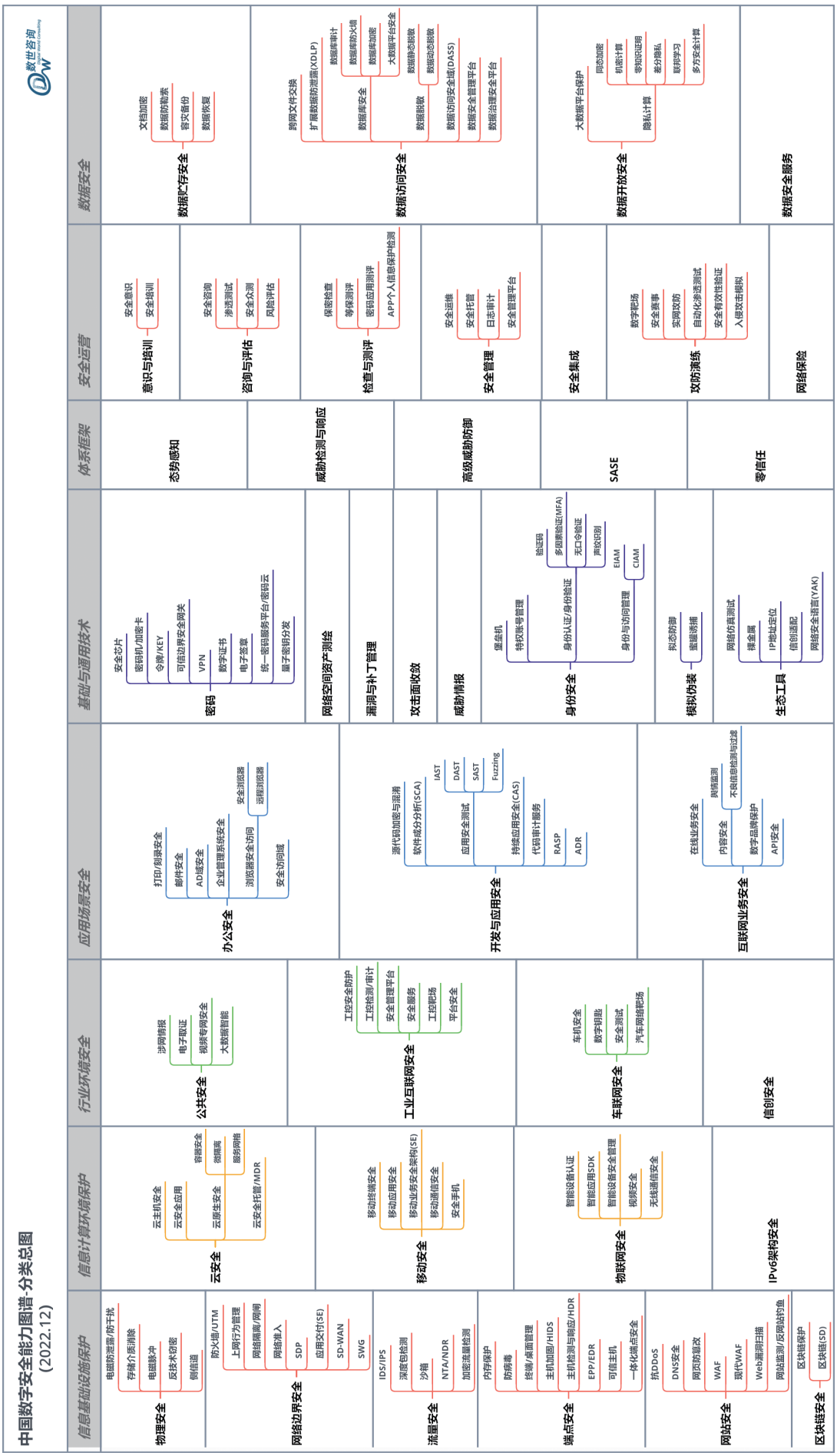


图 19　数字安全能力图谱总分类

1、政府部委

信息基础设施保护	**网络边界安全**	山石网科、启明星辰、新华三、天融信、深信服、信达网安
	流量安全	恒安嘉新、绿盟科技、奇安信、天融信、启明星辰、安恒信息
	端点安全	安天、奇安信、360数字安全、安全狗、天融信、绿盟科技 安恒信息、江民科技、安芯网盾
	网站安全	瑞数信息、绿盟科技、电信安全
信息计算环境保护	**云安全**	观安信息、安全狗、阿里云、知道创宇
	移动安全	盈高科技、梆梆安全
	物联网安全	天懋信息、慧盾安全、迪普科技、新华三、远望信息、世安智慧
行业环境安全	**公共安全**	美亚柏科、效率源、上海弘连
	工业互联网安全	奇安信、安恒信息、烽台科技、珞安科技、博智安全
应用场景安全	**开发与应用安全**	海云安、思客云、云弈科技
	互联网安全	通付盾、微步在线、恒安嘉新
基础与通用技术	**密码**	万里红、中孚信息、数字认证、飞天诚信、九州量子
	网络空间资产测绘	360数字安全、知道创宇、华顺信安、盛邦安全
	漏洞与补丁管理	斗象科技、默安科技、华云安
	攻击面收敛	烽台科技、华顺信安、天懋信息、云科安信
	威胁情报	微步在线、天际友盟、奇安信、360数字安全
	身份安全	派拉软件、竹云、芯盾时代、齐治科技
	模拟伪装	永信至诚、锦行科技、经纬信安、长亭科技、默安科技
体系框架	**态势感知**	深信服、奇安信、启明星辰、新华三、绿盟科技、安恒信息
	威胁检测与响应	安天、火绒安全 、奇安信
	高级威胁防御	安天、安恒信息、天融信、深信服、奇安信、绿盟科技
安全运营	**意识与培训**	红山瑞达
	安全管理	安信天行、联成科技、远禾科技、安恒信息、天融信、深信服 奇安信、绿盟科技
	安全演练	永信至诚、赛宁网安、丈八网安、安码科技、锦行科技、博智安全
	网络保险	嘉韦思
数据安全	**数据贮存安全**	世平信息、海峡信息、美创科技
	数据访问安全	闪捷信息、明朝万达、天融信、赛猊腾龙

图 20　政府部委

基于分类分级的数字政府数据安全流转监测与防护方案

闪捷信息科技有限公司

【用户需求】

数字政府是推动数字中国建设的重要支撑，安全作为发展的伴生体，为应对新时代数据安全风险挑战，政府行业的数据安全防护必须高度重视。数字政府建设过程中，存在组织机构数据分类分级能力较弱、可用数据分类分级信息滞后、内容识别技术准确度低、数据安全风险监测能力欠缺等痛点。因此，亟需对域内数据进行摸底盘点、分级分类、关联分析、风险评估等综合安全治理，实现数据全生命周期安全管理，确保数据来源可信、访问可控、操作可查和责任可追。

【解决方案】

（一）数据安全分类分级服务

发挥数据安全分类分级起承上启下的作用，完成迈向数据安全精细化管理重要一步。承上：运维制度、保障措施、岗位职责等多方面的管理体系都需依托数据分类分级进行针对性编制。启下：根据不同数据级别，实现不同安全防护。工作流程包含分类分级方案预研、分类分级方案确定、分类分级方案评审三个环节。

（二）数据安全资产管理系统

数据分类分级方案确定后，引入自动化工具，采用“工具”+“人工”的方式对数据进行分类分级标识，加速项目实施速度，降低错误率，为企业或组织构建数据安全运营体系打下夯实的基础。系统分为数据资产探测、数据资产梳理、敏感数据识别、数据分类分级、数据资产多维分析等功能模块，同时采用 AI 技术提升内容识别的准确性与识别工具的实用性及应用范围，以达到数据资产“可见、可懂、可控、可用”。

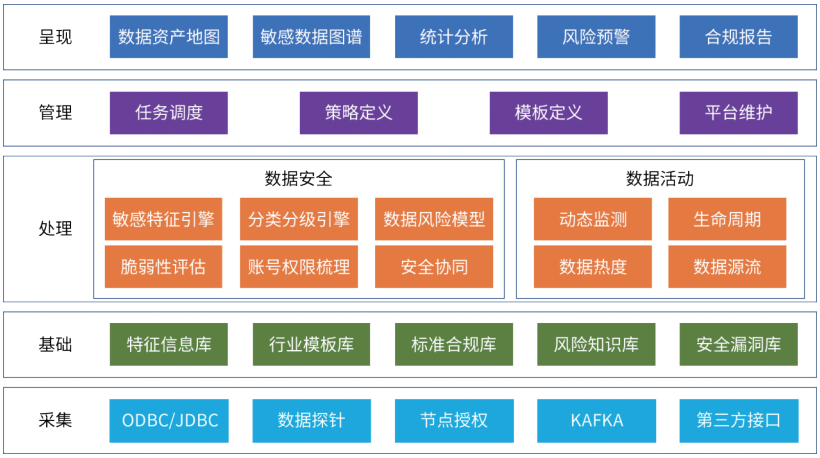


图 21　数据资产管理系统逻辑架构图

（三）与数据安全产品联动

将分类分级信息与数据安全产品联动，实现敏感数据信息与安全风险等内容的实时同步，形成有针对性的数据安全防护策略，实现加密、脱敏、审计、访问控制等的策略协同与联防联动。

（四）直观可视、可查、可判、可用

根据分类分级结果，自动监测敏感数据的流动和访问情况，在风险识别模型基础上采用 AI 技术提升风险识别能力。支持广泛的数据源类型及常见非结构化数据资产识别，自动化生成统计报表，提高常态风险管理能力与数据安全风险监测能力。

【用户评价】

该建设项目采用政务行业的数据识别规则模板和 AI 技术，识别的自动化程度达到 96%，根据数据梳理结果制定出差异化的安全策略，优化了安全资源配置，整个防护体系统一管理，策略共享，防护无遗漏。建设系统自身不存储、不截留用户的真实业务数据，确保用户业务数据在维护、管理过程中不会曝光和泄露。该项目为数字政府行业数据安全防护提供了新的治理模式，具有良好的示范效应，为数字政府建设和数字经济发展提供了行之有效的安全保障。

某人力资源和社会保障局电子社保移动安全建设案例

北京梆梆安全科技有限公司

【用户需求】

近年来，电子社保卡业务一直在不断创新，由之前人社范围内的一卡通办到目前实现支持更多政务数据的一卡共享、各类民生服务的一卡多用。人社部重点搭建完善服务内核，以将内核嵌到地方政府 APP 及各大银行 APP 中，方便广大群众使用电子社保卡。由于社保数据的特殊性，它已成为个人隐私信息泄露的“重灾区”，如被公开售卖，用于牟利，社保行业的安全建设面临严峻的风险与挑战：

- 防范个人隐私信息泄露
- 社保数据防护能力提升
- 符合社保行业移动安全合规要求

【解决方案】

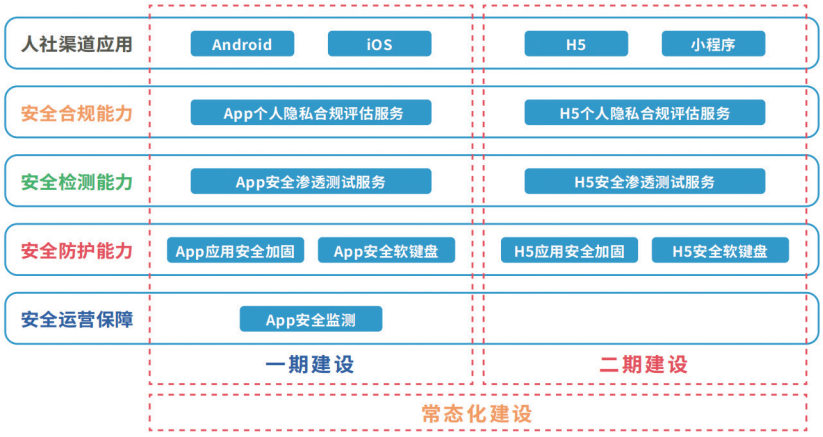


图 22　解决方案示意

基于社保移动端的安全态势及行业政策，梆梆安全社保移动安全解决方案，防护对象包括 App 和 H5 小程序，方案覆盖安全合规、安全监测、安全防护以及安全运营保障四大框架。根据人社移动端安全建设任务的紧迫程度，建议分期进行建设。

一期建设

App 是社保业务的重要承载渠道，作为安全合规检查的重点对象，一期建议优先构建 App 端的安全防护措施及安全运营保障。

安全防护措施

应用安全加固：有效防止针对智能应用软件的逆向分析、二次打包、内存注入、动态调试、数据窃取、界面劫持、应用钓鱼等恶意攻击行为，使客户端具备基本的抗攻击能力，全面保护智能应用软件安全。

App 安全软键盘：通过梆梆安全独有的白盒加密技术对密钥进行保护，使用严格的加密方式对用户输入的信息进行安全处理，并提供多种类型的输入字符供用户进行切换，降低了输入数据泄露的风险，保障客户端信息输入的安全。

安全运营保障

App 安全监测：保障客户端的环境校验，检查客户端运行时所必须的条件，确保客户端自身和所处运行环境的安全性。通过对移动应用运行过程的持续监控，从动态攻击的技术源头进行感知分析，提供多维度的安全态势统计，并以可视化图表的方式展现整体安全形势，帮助用户快速建立事前、事中、事后的移动应用安全监测防御体系。

二期建设

H5 安全加固：有效防止针对 H5 Web 应用、H5 混合应用、小程序、公众号进行的反编译、动态调试、代码篡改、JavaScript 盗用等攻击行为，降低因 H5 自身安全缺陷带来的各种风险，使 H5 页面具备基本的抗攻击能力。

H5 安全软键盘：保障 H5 小程序端信息输入的安全，为开发者提供高强度数据加密保护能力，同时支持展示企业 Logo、安全软键盘等信息，让用户在输入过程中意识到被保护,提升用户对企业安全服务能力的认可和品牌认同感。

常态化建设

个人隐私合规评估服务：根据客户提供的行业合规要求，帮助企客户在监管部门检查前自查自纠，提前发现问题，确保其符合行业安全合规、个人信息合规要求，保障服务渠道在采集用户个人敏感数据时的合规性。

安全渗透测试服务：利用漏洞产生原理和渗透测试方法，通过黑盒方式对各类信息系统及应用等进行深度弱点探测和脆弱性测试，帮助应用开发者和管理者了解应用系统存在的脆弱性，为改善并提高应用系统安全性提供依据和解决方案，保障服务渠道避免由软件漏洞引发的安全风险，帮助用户建立安全可靠的应用服务。

【用户评价】

感谢“梆梆安全”投入大量人力物力，为项目顺利推进提供了有力支持。在移动安全建设项目中，项目团队与我单位积极配合，工作负责，业务精湛，展现出很好的工作能力和作风。

2、金融

信息基础设施保护	**网络边界安全**	信安世纪、新华三、山石网科、华为、奇安信
	流量安全	启明星辰、绿盟科技、新华三、奇安信、斗象科技、科来网络
	端点安全	奇安信、安天、联软科技、亚信安全
信息计算环境保护	**云安全**	青藤云安全、小佑科技、默安科技、瑞数信息 全知科技、探真科技、安全狗
	移动安全	指掌易、爱加密、安软信创、梆梆安全 、联软科技、嘉赛信息
	物联网安全	万物安全
应用场景安全	**开发与应用安全**	悬镜安全、海云安、开源网安、默安科技、云弈科技 国舜股份、酷德啄木鸟、边界无限、火线安全
	互联网安全	顶象科技、国舜股份、芯盾时代
基础与通用技术	**网络空间资产测绘**	360数字安全、斗象科技、魔方安全、云弈科技
	漏洞与补丁管理	斗象科技、默安科技、华云安、碳泽信息
	攻击面收敛	华顺信安、未来智安、安博通、360数字安全、华云安 零零信安、魔方安全
	威胁情报	微步在线、奇安信、360数字安全
	身份安全	芯盾时代、竹云、派拉软件、齐治科技
	模拟伪装	默安科技、长亭科技、元支点、360数字安全
体系框架	**态势感知**	奇安信、启明星辰、天融信、深信服
	威胁检测与响应	未来智安、兰云科技
安全运营	**意识与培训**	易念科技
	检测与测评	嘉诚信息、北方实验室、赛可达实验室、时代新威
	安全演练	360数字安全、默安科技、奇安信、绿盟科技
	网络保险	嘉韦思、众安科技
数据安全	**数据贮存安全**	安华金和、炼石网络、安恒信息
	数据访问安全	天空卫士、明朝万达、闪捷信息、北信源、数安行

图 23　金融行业

斗象科技 VMS 漏洞运营管理系统某商行联盟解决方案

上海斗象信息科技有限公司

【项目背景及需求】

某商业银行合作联盟有限公司（以下简称“联盟”）基于业务的发展与安全建设需求，每年定期开展渗透测试、上线安全评估检测、攻防对抗演习等工作，因此其内部汇集了大量的安全漏洞数据，这些数据仅能通过人工统计、排重后在进行后续漏洞的重新汇总、分发、处置修复等工作。但随着业务系统投入数量的增长，沉淀的漏洞数量与日俱增，传统的表格及邮件管理的模式已无法满足漏洞生命周期管理的要求且零散、繁多的漏洞、报告等数据统计的不完整、处置流程偏向于原始的漏洞处理方式等因素，不仅导致内部漏洞处理效率低下，同时沉淀的大量漏洞数据潜藏价值效能无法发挥，也难以转化为联盟自身的安全能力。

在此背景下，联盟急需能够提供标准科学化的漏洞运营管理平台，实现综合漏洞数据的全面管控，同时建立起联盟自有的漏洞库和知识库，不断沉淀并扩展其价值并为后续的漏洞治理运营工作奠定基础。

【解决方案】

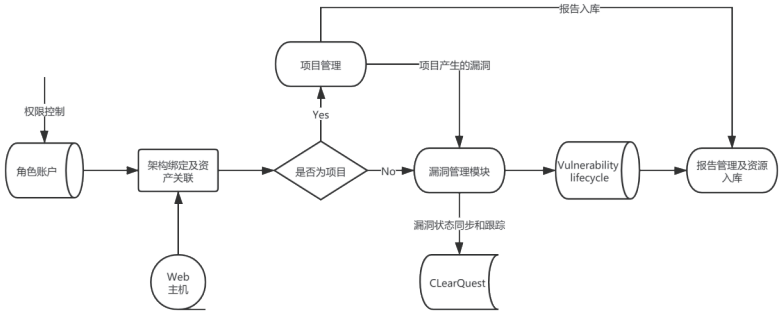


图 24　联盟漏洞管理平台流程示意

为有效实现管理及沉淀漏洞资源，上海斗象信息科技有限公司（以下简称“斗象科技”）以自研漏洞运营管理系统为基础，通过其内部的流程化、体系化、

持续化的漏洞运营机制，结合系统内置的漏洞全生命周期管理办法，为联盟建立起完善且符合实际需求的漏洞运营管理平台及漏洞全链路治理解决方案。该平台由联盟技术管理部负责使用，VMS 漏洞管理运营系统平台使用主要作为部门内部的漏洞管理、漏洞修复、漏洞验证、漏洞归档等流程开展。

租户分权分域，实现精准且安全的权限管理

基于联盟内部的资产庞杂极难统筹管理问题、部门权责等情况，VMS 漏洞运营管理系统内置以角色为主的权限划分机制，为联盟专项设计了一套逻辑化的内部职能划分的体系架构，实现了资产、架构、角色、账户等维度的逻辑设置，帮助内部漏洞管理对接工作的高效串联。

模型可扩展，实现漏洞管理流程的高度管控和灵活适配

VMS 漏洞运营管理系统内置漏洞审核、修复、复审、关闭的标准化漏洞管理方法，实现了对漏洞的生命周期管理。以项目需求为出发点，斗象科技为联盟设计出漏洞提交、审核、确认、整改、复测等关键节点的漏洞管理流程，以及项目对接管理机制，同时基于使用和变更的考量，VMS 漏洞运营管理系统引入后台流程配置引擎模块，用户可通过流程模板画布配置及表单自定义功能，构建起独有的符合用户需求的漏洞管理办法，完美契合联盟未来的发展及变更需求。

海量漏洞情报，助力漏洞运营的智能化决策

VMS 漏洞运营管理系统对接 CVND、CNNVD 官方漏洞库、CERT 和社区类漏洞库，整合运营海量安全漏洞情报，基于不同的业务场景，赋予系统智能化分析和决策能力。以联盟自有漏洞数据其基础，VMS 漏洞运营管理系统自定义字典模块帮助联盟构建起专用漏洞库,为后续的漏洞数据利用价值最大化提供支持。

此次项目，斗象科技 VMS 漏洞运营管理系统不仅帮助联盟构建起起科学完善的漏洞生命周期管理流程，摆脱了粗放式漏洞管理弊端，全面提升漏洞处置效率；同时帮助其打破内部数据孤岛，融合关键信息，实现漏洞运营一体化管理，协助其沉淀的漏洞数据内化，为联盟未来安全建设提供可靠参考和动力源泉。

【用户评价】

通过引入斗象科技 VMS 漏洞运营管理系统，极大缩减了我们漏洞发现和修复的时间，降低漏洞资产被攻击概率，斗象科技提出的漏洞运营治理解决方案，不仅帮助我们建立更快速、更集中化地漏洞收集、流转、处置类平台，同时在长期的运营管理过程中，给予科学的治理优先级理念，指导未来联盟安全漏洞管理工作，大大提升了管理人员的运营效率。VMS 的漏洞知识库功能，也帮助我们构建起漏洞数据汇入，库内漏洞数据内化，高价值漏洞案例沉淀形成知识闭环，为未来的人才培养奠定了知识的基础。

某大型金融机构行业案例

北京指掌易科技有限公司

【客户需求】

近年来，云计算、人工智能和 5G 等新技术广泛应用，给金融机构在数字化转型建设、运营效率等方面提供了基础条件。并随着智能终端设备的种类、功能不断丰富，某大型金融机构顺势实现了业务应用和办公应用的移动化，新增了混合办公、移动展业和移动营销等多个移动化场景。

移动化不仅给员工带来了便捷性，流程处理、外出走访和移动办公等效率也有了极大地提升。但是在方便员工访问移动应用服务和数据资源的同时，对外开放的服务端口有增无减，存在来自互联网的恶意攻击活动。碎片化的移动设备接入和使用，仍然出现非法泄露、账号被盗用和冒用等安全问题。在个人自带终端上进行远程办公，工作数据无意识的留存、转发分享、恶意程序窃取导致泄露等情况经常发生。针对该金融机构的现状，打造一体化、多场景的移动化安全管理平台，适应于手机、PC 端和信创终端等多种设备环境使用，同时兼具较好的用户体验。

【解决方案】

某金融机构现有员工 5 万多人，不同类型的应用，根据系统属性、用户范围、数据敏感性等在多个网络中部署。该金融机构根据未来战略计划和科技发展规划，整体网络架构，结合移动安全场景的需求，采用以全局视角设计全场景、按需弹性扩展的指掌易移动化安全解决方案。

整体解决方案采用了终端安全沙箱、SDP 和 MFA 等关键技术，适用于金融机构的办公、展业、开发和运维管理等场景，提供用户可信接入控制、终端应用和数据保护、收敛互联网暴露面、数据传输安全等安全能力。

根据金融机构办公终端设备类型，提供安卓、iOS、鸿蒙、Windows、

MacOS 和信创等跨平台终端的安全沙箱，办公应用和数据在沙箱环境中运行，增加水印、防止截屏、限制转发和数据加密等防泄露保护。对应用提供单点登录、应用预置和客户端调用能力，确保安全、稳定且简单易用。针对配发展业设备统一管理，推送、安装展业应用，根据相关政策要求，审计记录设备使用行为。

建立“以身份为中心”的零信任体系，通过 SDP 的两个核心组件，将控制面和数据面分离，由 IAM 提供多因素认证和统一身份管理，全面落实零信任“从不信任 - 持续验证”的理念。该金融机构所有接入的终端设备先认证后连接，确保用户、设备和环境可信接入，最小化授权资源访问，以及安全通道数据加密传输。同时，应用服务端口不再直接向互联网暴露，隐藏在 SDP 之后。

在 OA 网、生产网、研发管理区以及子公司网络 6 个相互独立隔离的网络中，采用集群高可用方式部署于同城双数据中心。一体化安全管理平台，提供用户、设备、安全策略和日志报表等可视化管理。截止目前，现有已将 30 多个 APP、B/S 和 C/S 等办公业务应用通过指掌易平台提供安全可信接入和数据防泄露保护。

【用户评价】

指掌易安全管理平台上线 2 年多时间以来，原来向互联网开放的办公业务应用服务实现了隐藏，被攻击的频率明显减少。长期存在的社工、网络钓鱼等攻击手段，结合产品安全策略配置，得到有效抑制。近期，我行持续参与第三方的多次攻击演练活动，有效抵御了各类攻击。在安全性方面得到了验证，达到了预期目标。

接下来，我行陆续将办公、业务应用基于指掌易平台使用，业务模式也不再依赖于以往的指定配发设备，逐步推广“全员营销”加速业务发展。整体产品方案，值得投入建设和推广使用。

某全国性股份制商业银行移动安全建设案例

北京梆梆安全科技有限公司

【用户需求】

随着各种利用 Web 应用漏洞进行攻击的事件正在与日俱增，各类拟人化自动化攻击、API 业务攻击、0day 攻击对金融数字化业务的影响也在快速攀升，攻击手段愈发多元化,移动应用安全已经成为金融行业数字化进程的重中之重。

数据驱动的金融业务创新对网络安全规划和建设提出了更高要求

金融行业数字化转型带来了资源开放和共享，使数据更容易以转存、截屏、分享等方式被外发，或因终端丢失等原因导致数据泄露，资产暴露面变大，受攻击维度增多。金融数据的交互、传输、共享等往往有多方参与，数据泄露风险点激增，风险环境愈发复杂。

金融科技数据安全风险防范和隐私保护难度加大

《个人金融信息保护技术规范》《金融数据安全 数据安全分级指南》《金融业数据能力建设指引》《金融数据安全 数据生命周期安全规范》《证券期货业数据安全管理与保护指引》等行业监管政策和标准陆续发布实施，金融业强化数据应用的安全性与合规性迫在眉睫。

传统静态安全防御已无法满足金融科技网络安全需求

随着科技与业务深度融合，延伸出隐私加密、人脸识别绕过、高级威胁攻击等新的安全问题，传统的金融服务模式已经不能匹配最新的数字化需求。

数据多接口开放，API 易被利用成为数据泄漏源

API 作为驱动开放共享的核心能力，已深度应用于金融行业；与此同时，其巨大的流量和访问频率也让数据安全风险面变得更广、影响更大，同时由于其固有的可访问性，成为了网络犯罪团伙的完美目标。

【解决方案】

梆梆安全基于已有的威胁情报数据、快速变化的业务场景、金融行业的客户积累，从不同场景的个性化需求出发，已形成基于热点场景的移动安全全栈解决方案。

移动安全建设矩阵

保护方法

保护对象	安全组件	自动化安全检测工具	合规检测工具	安全加固	安全监测	盗版仿冒监测	API安全监测	渗透测试	个人隐私合规服务	移动攻防安全能力提升
Android APP	基础	完善	提升	基础	完善	基础	提升	基础	基础	提升
Android外发SDK	基础	完善	提升	基础	完善	不涉及	提升	完善	基础	提升
Android引入SDK	基础	完善	提升	不涉及	完善	不涉及	不涉及	完善	基础	提升
iOS APP	基础	完善	提升	基础	完善	不涉及	提升	基础	基础	提升
iOS 外发SDK	基础	不涉及	提升	基础	完善	不涉及	提升	完善	基础	提升
iOS 引入SDK	基础	完善	提升	不涉及	完善	不涉及	不涉及	完善	基础	提升
H5	基础	不涉及	提升	基础	提升	不涉及	提升	完善	基础	提升
小程序/轻应用	基础	完善	提升	基础	提升	不涉及	提升	完善	基础	提升
	开发阶段（编码）	开发阶段（测试）		发布阶段	运维阶段			人工服务		
	移动安全全流程安全保障：产品、平台、服务、流程									

图 25　移动安全建设矩阵

人脸识别绕过

从人脸识别绕过看技术与业务双轮驱动的风控升级，实现对“人脸识别”绕过等安全风险的监测并将其落地。预防，减少攻击风险；事前，提高攻击门槛；事中：实时监测状态；事后：攻击事件溯源。

屏幕共享电信诈骗

安全键盘 SDK 可以防基于远程会议系统共享屏幕的信息泄露，同时，为了保障中老年用户的使用安全，可以定义按键时是否发音或震动。以避免防录屏这种模式下，用户的无感知操作导致的误操作；移动安全监测具备：①应用破解检测、②异常使用手段检测、③运行环境风险检测等关键技术能力，针对 APP 前端建立长效的监测防御机制。

个人隐私合规保护

基础性保障（快速合规，短期内不被通报）+ 建设性完善（常态化个人信息保护合规评估服务）+ 安全合规基线化落地（长期的自生安全合规能力沉淀）。

移动自生安全能力建设

移动安全能力平台赋能企业人员移动安全攻防能力，为移动新业务场景、新技术业务场景提供最佳安全实践和经验。

拟人化攻击电信诈骗

API 安全平台与传统的移动安全产品联动，将客户端环境与服务端流量相结合，解决客户 API 面临的安全风险，有效的形成完整的闭环解决方案，真正形成 1（客户端）+1（服务端）＞ 2 的效果。

【用户评价】

我行非常注重自身移动安全体系的完善，采购梆梆安全的移动安全监测平台，以平台为抓手在网络安全攻防演练中取得了好成绩，并与应用加固等静态安全手段形成防御闭环，有效增强移动安全风险监控预警和溯源响应能力。个人信息合规检测平台、API 安全平台以及移动安全能力平台将持续为我行在 API 风险管控、个人信息合规检测能力以及移动安全自生能力等方面贡献价值。

3、运营商

信息基础设施保护	**网络边界安全**	华为、迪普科技、新华三、深信服、奇安信、信安世纪
	流量安全	华为、新华三、迪普科技、奇安信、科来网络、斗象科技 安博通、恒安嘉新、武汉绿网
	端点安全	亚信安全、绿盟科技、天融信、安天、安恒信息
	网站安全	云盾智慧、华为、迪普科技、新华三、网宿科技
信息计算环境保护	**云安全**	观安信息、瑞数信息、山石网科、绿盟科技、亚信安全 、安全狗
	移动安全	梆梆安全、爱加密、联软科技
应用场景安全	**开发与应用安全**	默安科技、悬镜安全、孝道科技、软安科技、酷德啄木鸟
	互联网安全	观安信息、瑞数信息、恒安嘉新
	办公安全	保旺达、思维世纪
基础与通用技术	**密码**	新华三、华为、信安世纪
	攻击面收敛	天懋信息、安博通、未来智安、观安信息
	网络空间资产测绘	魔方安全、华顺信安
	威胁情报	微步在线、奇安信、360数字安全
	漏洞与补丁管理	斗象科技、默安科技
	身份安全	竹云、派拉软件、亚信安全、保旺达
	模拟伪装	观安信息、默安科技、长亭科技、元支点
体系框架	**态势感知**	亚信安全、启明星辰、天融信、深信服
	威胁检测与响应	中科网威、启明星辰、绿盟科技、天融信、未来智安、兰云科技
安全运营	**安全管理**	安全狗、安恒信息、深信服
	检测与测评	竞远安全、赛宝认证、深圳网安
	安全演练	赛宁网安、四叶草安全、丈八网安、博智安全
数据安全	**数据贮存安全**	安华金和、闪捷信息、炼石网络
	数据访问安全	明朝万达、天空卫士、北信源、天融信、思维世纪、世平信息

图 26　运营商

4、公安

信息基础设施保护	**物理安全**	万里红
	网络边界安全	天融信、深信服、奇安信、启明星辰、腾讯安全、世安智慧
	流量安全	安天、恒安嘉新、奇安信
	端点安全	绿盟科技、青藤云安全、安恒信息、奇安信、深信服 安芯网盾、安全狗、天融信
	网站安全	阿里云、知道创宇、盛邦安全、网宿科技、腾讯安全
	区块链安全	知道创宇、成都链安
信息计算环境保护	**云安全**	腾讯安全、青藤云安全、知道创宇、深信服、安恒信息
	移动安全	明朝万达、天融信、奇安信、筑泰防务、创原天地
	物联网安全	慧盾安全、金盾软件、天防安全、迪普科技、盈高科技、世安智慧
行业环境安全	**公共安全**	美亚柏科、迪普科技、金盾软件、慧盾安全、天防安全 天懋信息、腾讯安全
应用场景安全	**互联网业务安全**	腾讯安全、美亚柏科、绿盟科技、恒安嘉新
	开发与应用安全	奇安信、安恒信息
基础与通用技术	**密码**	华澜微、三未信安、数字认证、吉大正元、格尔软件、中宇万通
	网络空间资产测绘	360数字安全、埃文科技、默安科技、云弈科技
	攻击面收敛	天防安全、天懋信息
	身份安全	安恒信息、奇安信、领信数科
体系框架	**态势感知**	安恒信息、奇安信、启明星辰、天融信、深信服
	威胁检测与响应	奇安信、安天、安恒信息
	高级威胁防御	安天、奇安信、中睿天下
安全运营	**安全管理**	安恒信息、奇安信、绿盟科技、启明星辰
	安全演练	永信至诚、烽台科技、奇安信、腾讯安全、安恒信息
数据安全	**数据贮存安全**	安华金和、慧盾安全、昂楷科技、美创科技
	数据访问安全	慧盾安全、安恒信息

图 27　公安

5、国防

信息基础设施保护	**物理安全**	中超伟业、中孚信息、博智安全、北信源
	网络边界安全	天融信、启明星辰、奇安信、电信安全
	流量安全	天融信、启明星辰、奇安信、安天、观成科技
	端点安全	北信源、奇安信、青藤云安全、江民科技
	网站安全	知道创宇、天融信、启明星辰
	区块链安全	北信源、知道创宇
信息计算环境保护	**云安全**	青藤云安全、奇安信、知道创宇、启明星辰
	移动安全	指掌易、北卡科技、奇安信、天融信、北信源
	物联网安全	格尔软件、天融信、启明星辰
行业环境安全	**公共安全**	美亚柏科、北信源、天融信
	工业互联网安全	博智安全、中电安科、天融信、启明星辰、奇安信
	车联网安全	天融信、奇安信
应用场景安全	**办公安全**	中超伟业、奇安信、航天启星
基础与通用技术	**密码**	吉大正元、天融信、格尔软件、中孚信息
	网络空间资产测绘	知道创宇、埃文科技、360数字安全、斗象科技
体系框架	**态势感知**	天融信、启明星辰、奇安信、深信服
	威胁检测与响应	奇安信、碳泽信息
	高级威胁防御	奇安信、安天、中睿天下
安全运营	**咨询与评估**	太极股份、奇安信
	检测与测评	中孚信息、安天
	安全管理	启明星辰、奇安信
	安全集成	太极股份
	安全演练	永信至诚、赛宁网安、丈八网安
数据安全	**数据贮存安全**	明朝万达
	数据访问安全	天空卫士、明朝万达、航天启星

图 28　国防

某国防客户安全监管解决方案

天翼安全科技有限公司

【客户问题和痛点】

由于安全监管平台建设工作要求，某国防客户需在短时间内推进二级单位安全监管平台全覆盖，加快集团总部及所属单位互联网出入口收敛，切实减少暴露面和风险点，初步形成基础设施一张网、资产态势一张图、安全监管一盘棋、风险管控一条线、产业服务一站通等支撑能力，实现国资央企网络信息安全能力水平整体提升。

【解决方案】

中国电信“天翼安全大脑”通过本地设备和云端分析平台的联动，实现云端安全分析服务＋本地安全攻击防御的双重安全服务，构建简单、高效、易用的安全云服务方案，降低安全分析工作的难度、提升安全运维工作的效率，从而降低客户在安全运维方面投入的成本，为客户提供新型的“可管理安全服务”。

中国电信天翼安全大脑面向有各类安全防护需求，但缺少安全控制管理手段的政企客户。中国电信天翼安全大脑基于网络安全运营平台，提供流量控制、入侵防御、攻击阻断、病毒查杀、上网行为审计等标准化安全服务，助力政企客户构建云侧运营分析、边侧威胁阻断、端侧贴身防护的云边端联动防护体系。

【技术原理】

中国电信天翼安全大脑服务平台作为整体方案的分析和服务中心，通过与安全网关联动，采集本地设备上报的全流量日志、安全事件相关告警数据，对数据进行二次分析，排除误报并分析出精准的安全事件，对于授权给云端进行自动处置的客户直接闭环安全事件；对于未授权给云端进行自动处置的客户产生处置建议，并将处置建议通过短信和邮件的方式发送给客户，从而完成安全服务的闭环。

【防护效果】

经济：高效构建一张广覆盖，快部署，高可靠，高安全的企业专用广域网。

可视：对全网链路流量进行可视化监控，全面掌握广域网链路流量和告警故障情况。

易管：在保障安全的基础上，提供最有性价比的组网方案，满足越来越高的带宽需求。

高效：能够远程管理，按需调度，统一规划，快速恢复，优化使用体验同时降低管理难度。

●中国电信天翼安全大脑上线后，完全满足合规要求，将互联网暴露面压缩到最低。

●众多二级／三级单位的设备，在总部统一维护，实时告警，在二级／三级单位无感知的情况下，完成业务切换。

【客户评价】

中国电信天翼安全大脑兼顾安全和组网，流量按需调度，从根本上解决了流量拥塞问题。我们可以通过小盒子很直观地看到设备状态，便于及时维护。背靠中国电信，电信安全所提供的运营商级安全服务确实出色，对比传统硬件堆叠的安全服务好很多，服务响应很及时，国资企业品质有保障。

6、能源

信息基础设施保护	**网络边界安全**	新华三、安盟信息、天融信、深信服、奇安信、启明星辰
	流量安全	科来网络、启明星辰、绿盟科技、新华三、天融信、奇安信、安天
行业环境安全	**工业互联网安全**	威努特、长扬科技、天地和兴、中电安科、珞安科技、六方云 网藤科技、烽台科技、启明星辰、天融信、奇安信
应用场景安全	**开发与应用安全**	默安科技、悬镜安全、思客云、绿盟科技、边界无限
	互联网安全	微步在线
基础与通用技术	**密码**	格尔软件、吉大正元、数字认证、中孚信息、江南天安
	网络空间资产测绘	默安科技、聚铭网络
	漏洞与补丁管理	安恒信息、奇安信、绿盟科技
	攻击面收敛	长扬科技、烽台科技、华顺信安
	威胁情报	微步在线
	身份安全	竹云、九州云腾、宁盾科技、芯盾时代
	模拟伪装	默安科技、经纬信安、斗象科技
体系框架	**态势感知**	绿盟科技、启明星辰、天融信、深信服
	威胁检测与响应	未来智安
	SASE	网宿科技
安全运营	**咨询与评估**	奇安信、太极股份、长亭科技
	检测与测评	中孚信息、安天
	安全管理	安恒信息、启明星辰、奇安信、绿盟科技
	安全集成	太极股份
	安全演练	永信至诚、烽台科技、绿盟科技、长扬科技、长亭科技 易霖博、软极网络
数据安全	**数据访问安全**	天空卫士、天融信、奇安信、启明星辰

图 29　能源

中国石油某销售公司油库网络安全改造推广项目案例

北京威努特技术有限公司

【用户需求】

油库是协调原油生产、原油加工、成品油供应及运输的纽带，是国家石油储备和供应的基地，它对于保障国防和促进国民经济高速发展具有相当重要的意义。为了油库生产网络的安全可靠运行，提出以下项目建设需求：

总体需要遵循中石油相关安全管理规定,参照等级保护以及安全基线要求，结合部署在总部数据中心系统和部署在库站系统的实际情况，制定有效的安全提升方案，落实网络安全负责主体，做到“组网清晰、外网防护、内网阻断、综合防护、统一管理”。

组网清晰：梳理网络架构、摸清家底，针对现有系统进行初步评估；

外网防护：油库生产系统主机设备禁止访问互联网；

内网阻断：实现生产网与办公网物理级别隔离，生产子系统之间实现逻辑隔离，网络边界处阻断非法请求、异常指令、攻击行为等；

综合防护：油库生产主机及服务器实现已知和未知病毒防护、安全基线加固、外设管控等，实现网络流量审计、工业业务行为审计；

统一管理：建立库级统一安全管理中心，实现库级工控网络安全设备集中管理、统一展示。

【解决方案】

安全服务

项目前期采用“ 调研 + 风险评估”的方式，针对 11 座油库进行细致的资产梳理、安全评估，从系统结构、要素、生命周期等方面确定调研及评估范围，采取文档查阅、现场访谈、现场检查等评估方法，最终协助客户识别资产约 400 点位，并对所有点位之间的网线、业务连接情况进行了梳理，绘制了 11 份与各座油库正在运行相符的拓扑图。识别 9 大类威胁、脆弱性问题 2000 余项、输出文档 30 余份，为后期的安全建设提供了第一手资料。

安全建设

借鉴中石油相关安全管理规定，参照等级保护以及指导方案要求，结合部署在总部数据中心系统和部署在库站系统的实际，制定了基于“行为白名单”的“纵深安全防御”技术方案，满足等保 2.0“一个中心、三重防护”以及中石油信息处规划总院的《销售工控系统安全防护指导方案》要求，进而构筑油库生产系统“安全可信环境”，确保：

- 只有可信任的设备，才能接入系统网络；
- 只有可信任的消息，才能在系统网络上传输；
- 只有可信任的软件，才允许被执行。

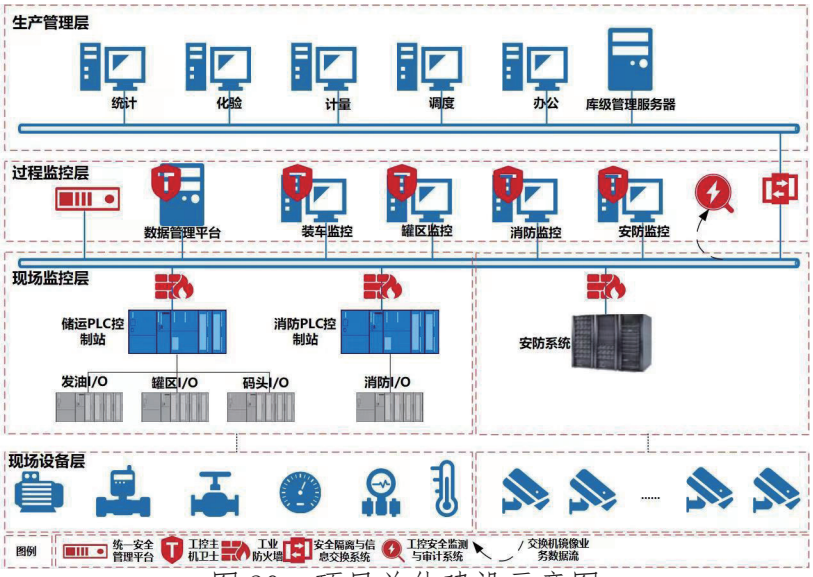


图 30　项目总体建设示意图

项目主要建设内容

为解决油库生产系统网络安全架构缺失，边界划分不清晰，没有合理的访问控制机制问题，将油库现场监控层的储运控制站、消防控制站以及安防系统分别划分为不同的安全区，并在安全区边界处串联部署工业防火墙，运用“白名单 + 智能学习”技术建立油库生产网络区域间通信模型，保证只有可信任的流量可以在网络上传输，为生产网络与外部网络互联、生产网络内部区域之间的网络连接提供安全保障；在过程控制层与生产管理层之间部署安全隔离与信息交换系统，在保障油库办公网与生产网之间数据安全交换的同时，最大限度保证客户应用的方便性；

为解决油库工控主机、业务服务器缺少安全防范机制问题，分别在数据管理平台服务器、装车监控主机、罐区监控主机、消防监控主机以及安防监控主

机上安装工控主机卫士软件，采用不同于传统防病毒软件的轻量级“白名单”机制，有效阻止包括 STUXNET、Flame、Havex、WannaCry、BlackEnergy 等工控恶意程序或代码在工控主机上的执行、扩散；

为解决油库底层生产业务网络缺少安全审计机制问题，在过程监控层的核心网络节点处旁路部署工控安全监测与审计系统，实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为油库生产系统的安全事故调查提供坚实的基础；

为满足等保 2.0 标准中对安全管理中心的建设要求，在过程监控层的核心网络节点处部署统一安全管理平台系统，实现对工业防火墙、工控主机卫士、工控安全监测与审计系统等工控安全资产的集中管理、安全策略的集中管控、安全事件的集中分析，提供油库安全态势分析，解决油库资产和安全运营可视化的难题。

【用户价值】

防护效果：项目建设完毕后，某油库销售公司邀请国家工信部渗透测试专家对油库生产网络安全建设效果开展了专项安全评估和渗透测试，测试均达到了油库生产网络安全防护的预期效果，为此石油销售公司致信感谢威努特。

经济效益：项目建设完成后全面提升某油库生产系统的整体安全性，保障油库生产系统的高效运行，同时减轻运维人员的工作量，提高了安全生产管理水平。

【客户评价】

由于该项目时间紧、任务重，且为了不影响油库的正常发油业务，项目组成员经常在夜晚油库不发油的情况下进行资产调研、线路梳理、网络切换等，放弃了多个节假日及周末的休息时间在用户现场加班工作。项目组成员不怕吃苦、认真负责的工作态度及专业的技术水平得到了我公司信息处领导及各个油库负责人的一致好评。在此，我公司对贵公司负责实施该项目的项目组成员表示衷心的感谢。

某干线天然气管道公司工控安全解决方案

杭州中电安科现代科技有限公司

【用户需求】

随着天然气管道企业信息化、管控一体化的建设与实现，越来越多的控制系统通过信息技术实现互联互通，使得工控系统网络架构愈发复杂，迫使内部的安全隐患逐渐暴露，工业控制系统网络安全问题日益突出，一旦各类生产系统遭受恶意攻击、勒索病毒等安全威胁，发生生产事故，将会直接导致经济损失、燃气泄漏甚至人员伤亡。

中电安科已帮助某干线天然气管道公司完成信息化建设，根据某干线天然气管道公司实际情况，结合《网络安全等级保护基本要求》、《网络安全等级保护安全设计技术要求》和《工业控制系统信息安全防护指南》等相关标准要求，科学合理评估某干线天然气管道 SCADA 系统合规差距和安全风险，确定安全保护措施，在此基础上设计了一整套完整的安全体系，以“一个中心、三重防护”为核心指导思想，从安全计算环境、安全区域边界、安全通信网络以及安全管理中心构建安全技术体系，满足等级保护第三级系统的相关安全要求。

【解决方案】

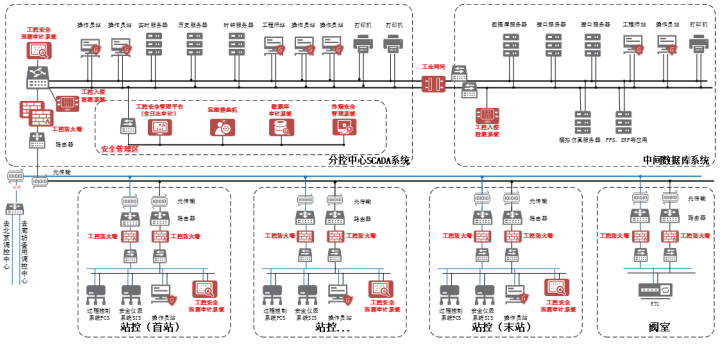


图 31　某干线天然气管道公司解决方案示意

（1）安全区域边界

调度中心在与站场控制系统、阀室等网络连接边界处要通过部署工控防火

墙进行边界防护，基于工控协议配置合理的主机访问规则，针对工业控制网络在同一个大网的情况，通过 ACL 等安全访问策略的配置对生产网络进行逻辑分区。

调度中心内部 SCADA 系统与中间数据库或管理信息系统之间，部署隔离工业网闸保证其安全性，除必须开放的用于数据交换的特定应用通道外，不提供任何对外的服务。

（2）安全通信网络

在工业交换机侧旁路部署工控安全监测审计系统，通过镜像接口分析网络中的网络流量，实现对工控网络中的网络流量进行采集、监测和分析，有效识别工控网络中的安全隐患、恶意攻击以及违规操作等安全风险。

（3）安全计算环境

通过在主机上安装终端防护代理程序,实现对工业主机的进程白名单管理，移动存储介质使用进行管理，有效抵御未知病毒、木马、恶意程序、非法入侵等针对终端的攻击，实现安全防护。

通过数据库审计系统实现对来自网络的数据库访问行为进行记录，及时判断出违规操作行为并进行记录、报警，为数据库系统的安全运行及事后审计提供有力保障。

（4）安全管理中心

通过工控安全管理平台，针对被防护资产综合全部安全要素信息，通过多种数据、分析方法构建动态的多层次、全天候网络安全管理，结合等级保护管理，为天然气管道构建网络安全动态深度防御体系形成对安全威胁、风险隐患的动态持续管理。

通过堡垒主机，实现运维单点登录，统一管理运维账号，管理运维授权，并对运维操作进行审计记录，并通过堡垒机实现对运维角色与权限的划分。

【用户评价】

有效提升了企业网络安全防护管理的合规性，符合国家主管部门、行业监管部门的管理要求以及工控安全防护要求。安全建设采用最低干扰方式，未对业务产生任何影响，通过可视化平台可清晰的看到生产网各节点的通讯情况，对资产的掌握情况大幅提升，通过本次安全建设实现了对生产网网络安全事件的事前预防、事中控制、事后可查，保障了天然气管道控制系统的安全运行。

7、电力

信息基础设施保护	**网络边界安全**	新华三、天融信、深信服、奇安信、启明星辰
	流量安全	科来网络
	端点安全	奇安信、安全狗、绿盟科技、天融信、云弈科技
行业环境安全	**工业互联网安全**	天地和兴、威努特、长扬科技、中电安科、启明星辰 天融信、奇安信、绿盟科技
应用场景安全	**开发与应用安全**	默安科技、思客云、绿盟科技、酷德啄木鸟
基础与通用技术	**网络空间资产测绘**	360数字安全、聚铭网络、斗象科技
	攻击面收敛	华云安、长扬科技、烽台科技
	威胁情报	微步在线、奇安信、360数字安全
	身份安全	芯盾时代、九州云腾、保旺达、申石软件、齐治科技
	模拟伪装	长亭科技、锦行科技
体系框架	**态势感知**	观安信息、深信服、安恒信息、奇安信
安全运营	**检测与测评**	竞远安全
	安全演练	烽台科技、永信至诚、博智安全
数据安全	**数据访问安全**	闪捷信息、华途信息、霍因科技、志翔科技

图 32　电力

电力新能源工控安全态势感知平台建设案例

北京威努特技术有限公司

【用户需求】

解决目前电力行业特别是具有集控中心的新能源企业普遍存在的工控系统信息安全孤岛、资产台账不全、无法集中管控等问题，针对可能面临的网络安全风险或正在发生的网络安全事件进行持续监测并及时预警，切实提升新能源场站关键信息基础设施的安全监测能力、态势感知能力和事件应急处置的数据支撑能力。

【项目内容】

通过对某新能源有限公司所涉及电力监控系统生产控制大区的网络安全监测（包括基于区域边界的安全监测、基于网络通信的安全监测和基于计算环境的安全监测），为集控中心工控安全态势感知平台提供支撑数据；完成新能源工控安全态势感知平台数据处理技术、数据智能分析技术和数据展示技术的创新研究，进而研发并建设一套具有新能源发电行业特色的工控安全态势感知平台，最终实现全国工控安全在线监测网络企业级节点的建设。

【解决方案】

项目整体秉承监测、防护、应急“三位一体”的理念开展建设。根据工控安全态势感知平台的数据采集需求，借鉴 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》的“一个中心，三重防护”的架构完成“一个中心、三重监测”的设计，同时为提高系统运维效率，将各新能源场站中新增的探针通过统一安全管理平台实现策略统一管理，监测安全设备的运行状态和策略的调整，包括：策略的增加、删除、修改等操作。此外，工控安全态势感知平台按照网络安全三同步原则，在不影响新能源场站现有设备、系统、网络等正常运行的情况下，充分考虑工控安全态势感知平台自身的网络安全等级保护要求。最终建成一套具备资产探测发现、多源数据采集、安全态势分析、安全

态势展示、告警分析处置、攻击溯源追踪、安全统计报表等功能的工控安全态势感知平台。

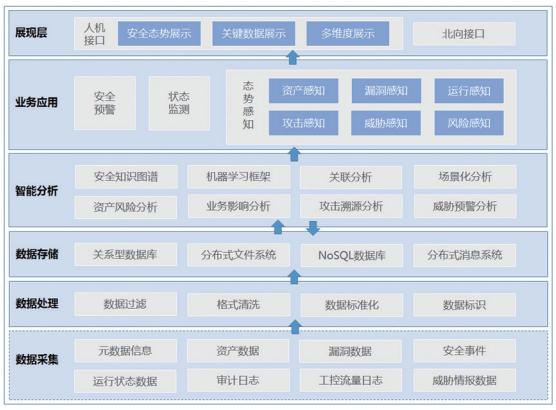


图 33

本项目通过深入的创新研究，技术水平已经达到国内领先；并取得了中国电力企业联合会颁发的科学技术成果鉴定证书。

●研发了工控数据库的安全审计分析技术。通过对工控数据库的全面审计，跟踪工控数据访问异常行为和违规行为，实现数据库行为建模、智能分析、态势感知、实时预警；

●研发了基于多视角报警融合的隐蔽攻击发现技术。通过提取资产信息、漏洞信息、拓扑信息等信息流特征和控制流程、能量信息、业务信息等物理流特征，实现了多视角报警；

●研发了基于知识图谱和机器学习的态势分析和威胁检测技术，采用数据挖掘算法提取攻击时间、攻击序列、攻击属性等特征，并依据上述特征构建工控网络攻击树，从攻击树中建立物理流与信息流映射关系；

●研发了工控网络安全健康指数评估体系。通过构建任务树模型和工业主机、网络边界、通讯网络的安全指数指标体系，准确识别与判定网络安全等级。

【应用效果】

工控安全态势感知平台的建成，解决了目前新能源企业普遍存在的工控系统信息安全孤岛、资产台账不全、无法集中管控等问题，实现了对网络资产和网络拓扑进行可视化发现、管理，能够监测网络安全防护措施和网络运行安全状态，能够对网络漏洞情况、合规配置、安全事件、网络威胁等风险进行监测

预警，提供了全方位、全天候的网络安全态势感知展示和事件应急处置的数据支撑；并通过使用成熟的主流大数据存储分析技术，将新能源场站的数据进行存储、处理和分析，将数据与集控中心进行对接，实现电力监控系统网络的安全威胁分析。

【用户评价】

本次项目实施阶段威努特项目组成员表现出了不怕苦，勇于克服困难，设身处地为客户着想的奉献精神，克服了严寒环境下室内外的复杂穿线环境，积极承担场站多个设备重新上架部署，在原有系统运行未受影响的情况下解决了场站设备无处安放的问题，提高了施工效率。施工过程中表现出了专业的技术水准，设备安装、网线敷设水平堪称一流，被定为样板，已在随后的项目施工过程要求按此标准执行。在此对本次项参加本次实施的项目组的辛苦付深表感谢，并提出表扬！希望贵公司继续保持优良的施工风范及服务理念，并衷心祝愿我们在今后的工作中能精诚合作共铸辉煌！

竞远安全电力行业网络安全综合服务案例

广州竞远安全技术股份有限公司

【服务内容及背景】

定制化网络安全综合服务，包含：等保测评、商密测评、风险评估、安全培训、应急响应等。

近年来，针对电力关键信息基础设施的网络攻击更加常态化、专业化，针对性极强，造成了大量的经济损失及社会影响。

为配合某电厂集团公司及电网完成 2022 年电力监控系统等保测评及安全防护评估等要求,需对某电厂生产控制系统开展等级保护测评(简称等保测评)、商用密码应用安全性评估（简称商密测评）及安全防护评估工作。

实施内容包含八套三级电力监控系统进行安全等级保护测评和安全防护评估，一套 DCS 系统商用密码应用安全性评估。

【用户需求】

专业可靠，资质齐全

客户更想通过相关的安全测评，真实有效的把单位的安全隐患展现出来，让客户未来更有针对性的开展网络安全管理工作，进一步增加网络和信息系统安全管理的规范性和有效性，提高单位的整体安全意识，增强网络抗攻击的能力，最大程度确保网络和信息系统正常运转。

技术过硬，高效服务

用户需要一家值得信赖同时具备等保测评、商密测评、风险评估、安全培训等资质的单位，出具的测评报告并能真实有效反应单位真实的安全隐患，促进整改，符合国家法律法规及监管部门的网络安全要求。与此同时，因招标流程及内部流程原因导致项目延误，用户亟需保质保量，高效完成安全测评。

【解决方案】

随着传统电力系统和信息化的深度融合，确保网络时代电力系统安全、稳定、高效运行和高质量供电始终是电力行业面临的重大考验。电力信息设施一般具有分布广泛、结构复杂、交互性强等特点，导致风险点多和接触面广，防护难度大，特别是关键电力调控中心、电网枢纽、核电站、大型火电、水电设施等重要目标一旦发生安全事件，后果十分严重，影响范围极大。

竞远安全依据合规治理原则设计，结合电力关键基础设施信息系统安全标准要求，为客户提供全流程的网络安全分类分级服务、等保测评、商密测评、数据安全评估服务，为客户开展安全培训，提高安全意识，助力客户开展网络安全合规建设与网络安全管理体系建设，明确数据分类分级、风险评估、安全认证、应急响应等关键制度规范要求。竞远安全为全国电力单位提供超过 100 套电力监控系统等级保护测评服务及安全防护评估服务，有用出色的电力行业融标能力。通过与其他电厂对比及对电力行业相关安全管理规范的解读，结合客户实际情况，与当地业务主管部门沟通交流，最终提出建议客户对八套系统合并进行专家评审，加速项目进程，提高工作效率。项目从 2022 年 11 月 12 日第一次进场实施到 2022 年 12 月 09 日完成交付，历时不到一个月时间，通过各部门紧密配合，顺利完成项目验收工作。

【用户评价】

竞远安全是国内为数不多的、同时具备等保测评、商密测评、风险评估、安全培训等资质的安全服务提供商，能够一站式解决我们的安全服务需求。且竞远安全实施团队非常专业，对我们的实际情况做了很深入的分析，急客户所急，会协助我们与主管部门反复沟通汇报，最终能在不到 2 个月时间内高质量、高效率完成了整个项目。

某省输电变电站

杭州中电安科现代科技有限公司

【用户需求】

输电变电站电力监控系统是国家关键基础设施，电力系统的安全运行与政治安全、经济安全、网络安全、社会安全等诸多领域密切关联，一旦发生大面积停电事件，可能引发跨领域连锁反应，导致重大经济财产损失，甚至引发社会恐慌，危及国家安全。

某省输电变电站已按照电力行业 36 号文规范，网络安全建设符合“安全分区、专网专用、横向隔离、纵向认证”要求，但在资产识别管理、流量解析与通信拓扑绘制、白名单基线与未知威胁 0Day 告警等方便比较欠缺，通过建设输电变电站流量监测预警与资产测绘，对电力监控系统网络流量采集、解析和分析，扩大现有安全监视的范围，对网络空间中异常资产及网络行为进行有效检测，提供回溯分析依据，从而提高电力监控系统网络安全防护水平，减少网络安全事件的发生。

【解决方案】

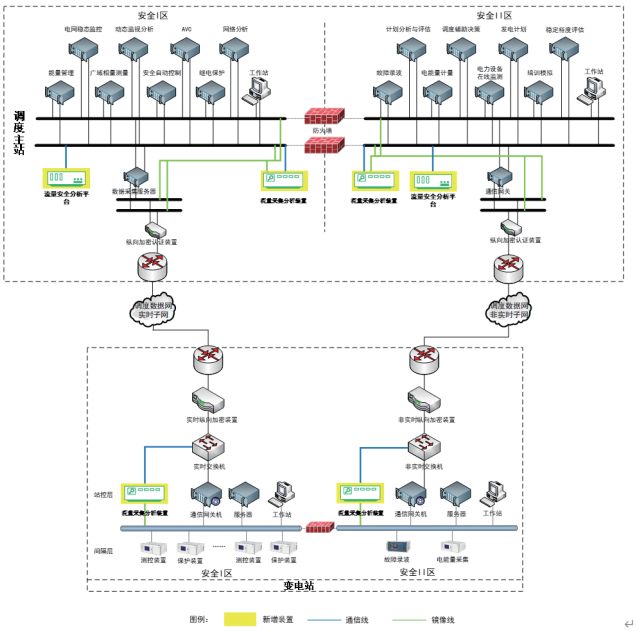


图 34

在输电变电站厂站Ⅰ/Ⅱ区分别部署流量采集分析装置，实现生产控制区内网络流量的采集、分析和存储，然后通过调度数据网将流量采集分析装置的数据上送到位于某省主站Ⅱ区部署的流量安全分析平台，实现输电变电站生产控制区流量数据的汇总集中监测与分析展示，有效识别网络中的安全隐患、恶意攻击以及违规操作等安全风险。

（1）采集各类常见的通用网络协议和工控协议，包括：数据链路层、网络层、传输层、应用层。重点对电力协议进行采集并深度解析，如：IEC103、IEC104、MMS、GOOSE/SV 等。各类协议流量按照流量特征格式或原始流量进行存储，对发生异常事件的流量片段进行标记存储。

（2）基于协议深度解析，对电力监控系统网络中的所有活动提供协议流量审计，生成完整记录并进行通讯行为识别。

（3）对网络流量实时分析，动态识别电力监控系统网络中的设备和属性，人工对资产的属性进行管理，包括名称、类型、厂商、IP/MAC、地理位置、联系人、资产登记等。

（4）内置流量负载规则库，对特征值进行分析匹配，及时发现流量的异常信息并进行告警，实现对组态变更，异常操控指令，程序下装等关键事件进行识别和告警，保证电力监控系统在正确配置下运行，如对 IEC61850 协议，IEC 104 协议等进行深度解析后，分析对应特定场景下的关键操作行为（遥控操作、改定值操作）等。

（5）通过对流量数据的学习，建立通信协议行为基线，识别异常的协议状态请求、控制协议指令；建立通信流量基线，监测通信链路、通信协议、持续时间、源与目的等特征的通信行为；建立通信链路基线，检测协议范围的流量、链路中断等事件。

（6）通过流量分析识别系统中所有通信链路，提供通信链路中的源/目的 IP、源/目的端口、通信协议、链路最早建立时间、链路最新通信时间、

包吞吐量等信息，自动以拓扑图的形式直观展示网络中各个设备节点之间的通信连接情况，对于存在入侵等告警信息的通信链路，在拓扑图上提供可视化的异常展示与告警。

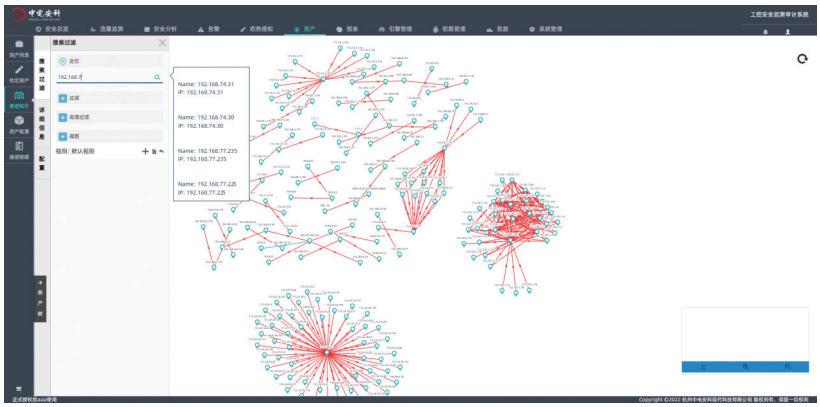


图 35

（7）提供基于规则的关联分析引擎，支持通过关联分析，从低风险事件中发掘高风险威胁的能力。

【用户评价】

输电变电站流量分析增强了二次安防流量检测方面的能力，规范了电力监控系统网络中的资产和行为，可以事前防御由病毒、入侵、异常接入、程序逻辑等导致的安全生产事故，杜绝重大灾难性事件，可以有效预警类似伊朗“震网”事件、乌克兰电网事件的恶意攻击。通过流量资产测绘提高了对省内分布数量众多的输电变电站的资产管理运维能力，网络行为分析实现了及时的安全事件预警，有利于保障输电调度的安全生产运行。

8、轨道交通

信息基础设施保护	**网络边界安全**	深信服、天融信、深信服、奇安信、启明星辰
	流量安全	启明星辰、绿盟科技、奇安信、新华三、天融信
	端点安全	奇安信、360安全、天融信、绿盟科技、火绒安全、安天
信息计算环境保护	**物联网安全**	锐捷网络、迪普科技
行业环境安全	**工业互联网安全**	中电安科、威努特、安恒信息、六方云、天地和兴、珞安科技 启明星辰、天融信、奇安信、绿盟科技
应用场景安全	**开发与应用安全**	默安科技、悬镜安全
基础与通用技术	**密码**	华澜微、万里红
	网络空间资产测绘	默安科技、魔方安全
	攻击面收敛	长扬科技、烽台科技、华顺信安
	身份安全	九州云腾、芯盾时代、申石软件
	模拟伪装	默安科技、长亭科技、经纬信安、非凡安全
安全运营	**安全演练**	博智安全、烽台科技、长扬科技
数据安全	**数据贮存安全**	明朝万达、华途信息
	数据访问安全	天空卫士、天融信

图 36 轨道交通

某城市轨道交通列车智能运维安全防护方案

杭州中电安科现代科技有限公司

【用户需求】

我国轨道交通行业列车（高铁、地铁）具有数量多、运量大、长期性、连续性和复杂性的运营特点，对列车车载系统安全性、可靠性和易维护性都有着越来越高的要求，同时《关键信息基础设施安全保护条例》于 2021 年 9 月 1 日正式落地实施，交通作为关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭受攻击的重点目标。面向快速发展的交通行业，列车车载系统需要将数据通过 LTE、无线 4G、5G 网络回传至地面，实现数据接入、数据处理、数据分析、数据显示等功能，同时将相关信息回显至司机室，在此过程中需要考虑车载系统车地通信的安全性。

某市轨道交通列车 TCMS 系统，负责对整列车各个子系统进行监测、故障诊断，以及为旅客提供信息服务。该系统会将车载系统的设备状态与故障数据通过主控制单元传输到司机室的显示屏并记录下来，让司机及时掌握车辆的运行状况，为了提升列车在线状态监测，将 PHM 数据通过车地无线通道进行落地，将相关数据传输到地面控制中心，同时保证地面系统被网络病毒感染后不会蔓延到列车上。

【解决方案】

分别在列车车头和车尾车载网络层设备，与无线系统及与车载外部其他系统之间部署车载防火墙，保障车地系统、车载系统与外部系统之间安全通信，实现车载业务系统的边界防护。

分别在列车车头和车尾车载网络层设备旁路部署车载监测审计系统，车载监测审计系统提供车载通信网络监测、协议分析和安全审计功能。实现车载资产可知、威胁可视，能够快速定位识别网络中的异常、攻击行为，并实时告警；同时记录所有网络通信行为，为车载系统的安全事故调查提供坚实的基础。

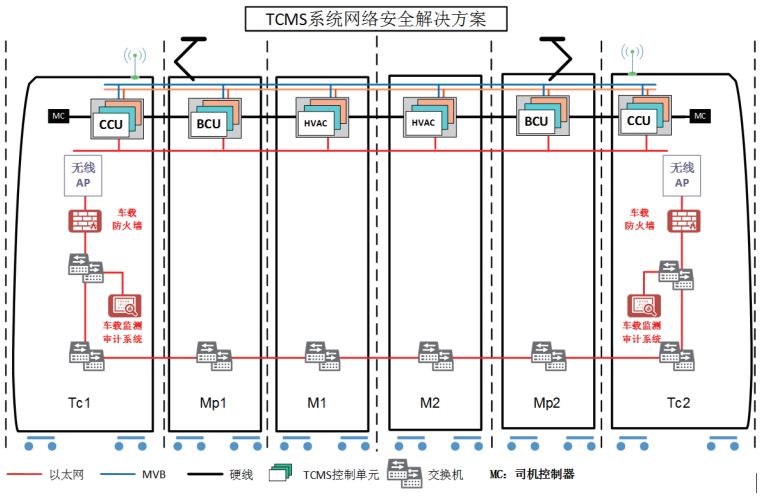


图 37　TCMS 系统网络安全解决方案

车载防火墙存活状态监测：车载防火墙通过 TRDP 协议定时发送存活数据值给车载主机，由车载主机判断安全设备的存活状态，能够及时的将设备状态信息展示在司机室。

车载防火墙时钟同步：车载防火墙接收车载主机发送的携带时钟信息的 TRDP 协议报文，进行时钟同步。确保在发生攻击、或威胁时方便关联追踪溯源。车载防火墙告警推送：车载防火墙将产生的告警通过 TRDP 协议推送给车载主机，车载主机会将告警信息推送至司机室，由司机依照告警类型、告警级别及告警内容进行相关处置。车载防火墙告警同时推送至安全日志管理系统进行展示和分析。

车载防火墙运维管理：通过车辆运维系统对车载防火墙进行运行维护，车辆运维系统与车载防火墙之间建立基于 HTTPS 及 SSH 访问的加密通道，实现车载防火墙的安全运维管理。

【用户评价】

在推动车载以太网快速应用落地过程中，为车载的 TCMS 系统安全稳定运行提供安全防护保障；能够对 TRDP 安全通信协议等进行深度的解析防护，有效的防止列车系统遭受攻击和网络病毒感染；直观的展示车载网络安全的威胁，

提高对安全威胁的应急响应能力，形成动态防御、监测预警、响应处置的安全运营机制，为车载系统的安全事故调查提供坚实的基础；实现事前预警、事中告警、事后审计的安全运维管理功能，提升车载网络安全的应急处理能力和管控能力。

某地铁集团 PSCADA 系统安全改造试点示范项目案例

北京威努特技术有限公司

【项目需求】

经过对某市地铁线路的评估调研以及和业主深入的沟通，本次项目建设重点应满足以下需求：

（1）通过等级保护测评，并满足国家网络安全部门三级等保要求，满足防范病毒入侵、黑客攻击、对数据有审计功能等技术要求的能力；

（2）整改过程中保持 PSCADA 系统既有功能和架构不受影响，串联设备故障情况下应确保业务可用；

（3）PSCADA 系统属于典型工业应用场景，应采用工控安全产品；

（4）建立安全管理中心，需实现安全设备统一管理、策略统一下发、设备监控等，汇聚交换流量收集与分析、预警，运维全程监控与审计等；

（5）应对网络中所有流量进行全面深度威胁检测与分析，强化新型网络攻击检测和分析能力；

（6）项目建设不能影响正常行车，需在夜间停电后施工。

【技术方案】

本项目依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，基于威努特多款白名单安全防护产品，并结合“一个中心、三重防护”的纵深防御思想，构建一套覆盖全面、重点突出、安全合规、持续运行的纵深安全防御体系。

安全区域边界

在控制中心与车站网络之间、车站变电所 PSCADA 系统与综合监控系统之间冗余部署工业防火墙，进行边界隔离和访问控制。工业防火墙对 PSCADA 系统 DNP 3.0 协议深度解析，建立访问控制白名单和 PSCADA 系统 DNP 3.0 协议白名单，构筑安全“白环境”边界隔离和控制防护体系。工业防火墙所有电口均支持 Bypass，从硬件设计上保证对业务系统“零”影响。

安全通信网络

在控制中心核心网络旁路部署高级威胁检测系统，接收核心网络交换机镜像流量，采用情报检测、入侵检测、行为检测、人工智能检测、病毒检测、基因检测和沙箱检测等技术，对已知和未知威胁流量进行深度包检测和分析，及时发现潜在的高风险威胁。

在控制中心核心网络旁路部署工控安全监测与审计系统，基于对 PSCADA 系统 DNP 3.0 协议的深度解析，实时监测网络内是否存在网络攻击、用户违规操作、非法设备接入等，结合“白名单 + 智能学习”机制实现 PSCADA 系统指令级审计，构筑安全“白环境”通信网络防护体系 。

安全计算环境

在 PSCADA 系统所有工作站部署工控主机卫士，设置程序白名单、网络白名单、外设管控、漏洞安全防护、强制访问控制等功能，锁定、切断恶意代码传播，强化主机层面网络和文件访问控制策略等，构建可信任的工作站级终端安全防护“白环境”。

图 38　工控主机卫士程序白名单展示

安全管理中心

●通过控制中心旁路部署的统一安全管理平台，对 PSCADA 系统中部署的工业防火墙、高级威胁检测系统、工控安全监测与审计系统、工控主机卫士等进行集中管理和策略统一下发；同时统一安全管理平台具备基于资产的风险分析功能，有效帮助业主提高 PSCADA 系统全面的安全态势感知能力。

●在控制中心旁路部署日志审计与分析系统，通过采集系统中主机设备、网络设备、安全设备、操作系统、数据库、业务系统的日志信息，对采集到的

不同类型的信息进行标准化处理和实时关联分析，协助安全管理人员从海量日志中迅速准确地识别安全事故，提高全面的安全管理、风险管理能力，同时也满足网络安全法对于安全日志留存 6 个月以上的要求。

●在控制中心旁路部署安全运维管理系统，统一对 PSCADA 系统下的所有资源设备运营和维护操作进行授权和管理，有效管控地铁运维人员、施工单位、设备厂商和第三方运维人员的操作行为。提供身份鉴别与认证机制，对不同身份用户操作进行严格的审计，从而提高 PSCADA 系统持续的安全运维能力。

●在控制中心旁路部署数据库审计系统，通过对地铁运维人员、施工单位、设备厂商和第三方运维人员和系统的网络行为进行解析、分析、记录、汇报，实现事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源的目的，从而达成加强内外部网络行为监管、促进核心数据库相关业务的正常运营目标。

●最后再提供漏洞扫描服务，定期对 PSCADA 系统安全防护措施的有效性进行全面扫描，并对识别出的漏洞给出修复建议，提升业主网络安全风险把控能力。

【客户价值】

安全合规：采用 2021 版测评模板和扣分算法通过等保三级测评；

对 PSCADA 系统“零”影响：除工业防火墙外，其余设备旁路部署；工业防火墙所有端口均支持 Bypass 功能，保证设备故障情况下业务可用性；

建立安全管理中心，实现了安全设备统一管理、策略统一下发、设备监控等，汇聚交换流量收集与分析、预警，运维全程监控与审计等目标。

【客户评价】

威努特深入研究城市轨道交通业务系统，针对性开发了诸多城轨专用网络安全产品，打造了适合城市轨道交通业务特点的一系列网络安全标杆案例，为城市轨道交通筑牢网络安全防线。威努特作为我司技术支撑单位，在以往项目中提供了功能强大的网络安全产品和优质的网络安全技术服务，展示了过硬的专业技术能力和认真积极的工作作风。

9、医疗

信息基础设施保护	**云安全**	山石网科、深信服、奇安信、天融信、启明星辰
	移动安全	指掌易、奇安信、联软科技、盈高科技
信息计算环境保护	**物理安全**	万里红
	网络边界安全	新华三、山石网科、华为、联软科技、奇安信
	流量安全	启明星辰、绿盟科技、新华三、奇安信、斗象科技
	端点安全	奇安信、安天、联软科技、亚信安全、阳途科技
	网站安全	绿盟科技、瑞数信息
应用场景安全	**开发与应用安全**	默安科技、孝道科技
基础与通用技术	**密码**	数字认证、吉大正元、三未信安
	网络空间资产测绘	聚铭网络、 默安科技、魔方安全
	身份安全	数字认证、吉大正元
	模拟伪装	永信至诚、观安信息、默安科技、非凡安全
安全运营	**意识与培训**	东软、安恒信息、奇安信、深信服、电信安全
	咨询与评估	
	安全集成	
	检测与测评	北方实验室、深圳网安、赛可达实验室、时代新威
	安全管理	联成科技、聚铭网络、华清信安
	安全演练	绿盟科技、长亭科技、默安科技
	网络保险	嘉韦思
数据安全	**数据贮存安全**	美创科技、亿赛通、安恒信息、安华金和、昂楷科技
	数据访问安全	慧盾安全、天空卫士、慢吉科技

图 39　医疗

10、互联网

信息基础设施保护	**网络边界安全**	深信服、天融信、奇安信、启明星辰
	端点安全	安全狗、长亭科技、云弈科技、绿盟科技、安芯网盾、青藤云安全
	网站安全	阿里云、电信安全、光通天下、长亭科技、缔盟云
	区块链安全	通付盾、慢雾科技
信息计算环境保护	**云安全**	腾讯安全、阿里云、长亭科技、青藤云安全、白山云
	移动安全	梆梆安全、指掌易
	物联网安全	梆梆安全、信长城
应用场景安全	**开发与应用安全**	孝道科技、默安科技、云弈科技、棱镜七彩
	互联网安全	顶象科技、威胁猎人、腾讯安全、通付盾
	办公安全	数篷科技、指掌易
基础与通用技术	**密码**	数盾科技、中孚信息
	网络空间资产测绘	360数字安全、默安科技、斗象科技
	漏洞与补丁管理	斗象科技、谋乐科技
	攻击面收敛	埃文科技、亿格云
	威胁情报	微步在线、天际友盟
	身份安全	九州云腾、宁盾科技、数字认证、吉大正元、信安世纪 芯盾时代、齐治科技
	模拟伪装	360数字安全、永信至诚、默安科技
体系框架	**零信任**	腾讯安全、数篷科技
	威胁检测与响应	华清信安
安全运营	**意识与培训**	圣博润
	安全集成	中国通信服务
	安全演练	博智安全、永信至诚、长亭科技、腾讯安全
数据安全	**数据贮存安全**	星瑞格、安华金和
	数据访问安全	天空卫士、明朝万达、亿格云、闪捷信息、数篷科技
	数据开放安全	阿里云、华控清交

图 40　互联网

某互联网行业客户移动安全建设案例

北京梆梆安全科技有限公司

【用户需求】

互联网为经济社会发展注入强劲动力的同时，也给世界各国主权、安全、发展利益带来许多新的挑战。侵犯个人隐私、侵犯知识产权、网络犯罪等问题时有发生，网络监听、网络攻击、网络恐怖主义活动等成为全球公害。如何发展互联网、用好互联网、治理互联网，已经成为国际社会面临的共同问题。

保障移动端业务安全

尽可能降低因网络攻击造成业务系统受影响的安全风险，例如移动端常见的的应用破解、盗版仿冒、恶意扣费、广告推送、植入病毒木马等。同时，能够掌控移动应用侧整体的安全态势，可主动发现潜在安全风险，及时知道谁、什么时间、做过什么样的攻击、攻击是否成功、移动业务系统受影响程度，并且在第一时间内解决遇到的安全问题。

企业上下游合作生态安全

对于外发的 SDK、API、H5，互联网企业普遍比较关心的安全问题集中在 4 个层面：1、是否存在潜在的业务逻辑缺陷，会被利用；2、发布后是否会被破解、逆向分析、盗版等；3、发布后是否会被非授权集成调用，导致管控机制失效；4、发布后是否会遭遇动态运行时攻击。

数据管理之安全合规

数据安全治理是所有互联网公司最核心的安全需求，也是绝大多数互联网企业高管最为关注的安全问题，其安全目标是要保障企业敏感数据的安全、可控。

国家层面的信息安全监管政策从顶层到执行、相互之间构成我国的信息安全监管体系，对互联网企业的生产运营从多方面做出明确要求，强制要求涉及网络运营服务的互联网企业必须进行网络安全法律合规体系建设。

解决企业内部自身安全

基于互联网企业的特点，其 BYOD 办公、业务移动化程度较高，保障接入安全、权限管控、内部应用安全、行为监测管控、企业数据安全等成为企业内部安全建设的重点。

【解决方案】

互联网行业需要从企业内部安全、业务安全、安全合规、供应链安全 4 个维度，构建动态、可持续的移动安全运管体系。

业务安全

围绕互联网企业 To C 端业务 APP，基于 SDL 框架，通过 APP 安全设计开发、安全测试、安全加固、安全监测、安全运营等产品技术，确保 To C 应用的安全合规。

内部安全

可通过 EMM（移动终端管理系统）对内部应用、内部文档、内网访问权限、身份认证、邮箱等进行统一安全管控，企业内部应用主要包括 OA、邮箱、财务、运维等业务系统；通过安全培训，培养和提升员工安全意识。

安全合规

通过自动化审计工具及人工审计服务，对 To C 端 APP 个人信息获取、权限使用等可能存在的合规问题进行发现与整改。

软件供应链安全

对于企业外发给第三方的 SDK、小程序代码等，除需要做好安全加固外，还需要通过安全监测手段，实时了解其安全态势，及时发现与处置安全威胁；对于企业集成的第三方 SDK、小程序代码等，在集成前，需对其安全性、合规性进行安全检测，避免因第三方合作机构出现安全问题而影响公司业务。

图 41

【用户评价】

我们非常重视移动端的安全建设，需要具备按需安全防护和快速威胁响应的能力。梆梆安全深耕移动安全领域多年，具备丰富的项目经验，从业务安全、内部安全、合规安全、供应链安全等多角度，覆盖我司核心业务系统，建立动态、可持续的运管体系，基于自动化、平台化的工具模块，进行高度的联动和关联分析，让我司能及时掌握移动端整体安全态势，面向用户输出安全能力，做到增值服务。

第五章　数字安全·资本

数字安全产业面向的是企业/机构级服务市场，尤其是在国内，与消费级服务相比，存在成长周期较长、市场十分碎片化、销售成本极高、定制化项目过多等困难，扩大规模几乎只能依赖不断拉长产品线。根据这些特点，数世咨询认为较合理的投资理念是“**长持有、多赛道、共成长**”。

——摘自《中国数字安全产业统计与分析报告(2022)》

国内的数字安全资本市场，自 2015 年之后连年持续速增，并于 2021 年达到顶峰，股权融资总额超过 150 亿元，融资笔数 180 余次。但在 2022 年出现急剧下滑，股权融资总额约 70 亿元，与 2021 年相比下降 56%。融资笔数接近百余次，与 2021 年相比下降 45%。

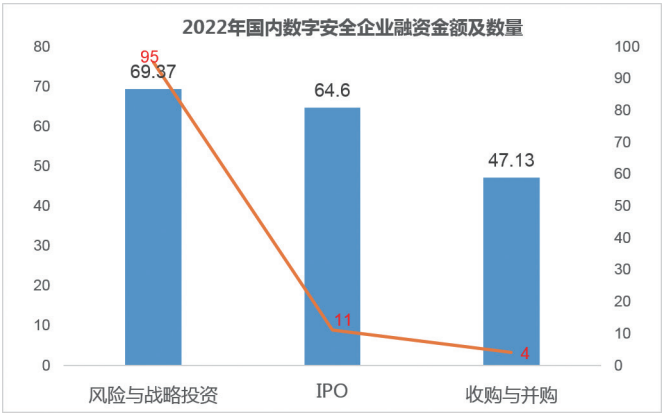


图 42　2022 年国内数字安全企业融资金额及数量

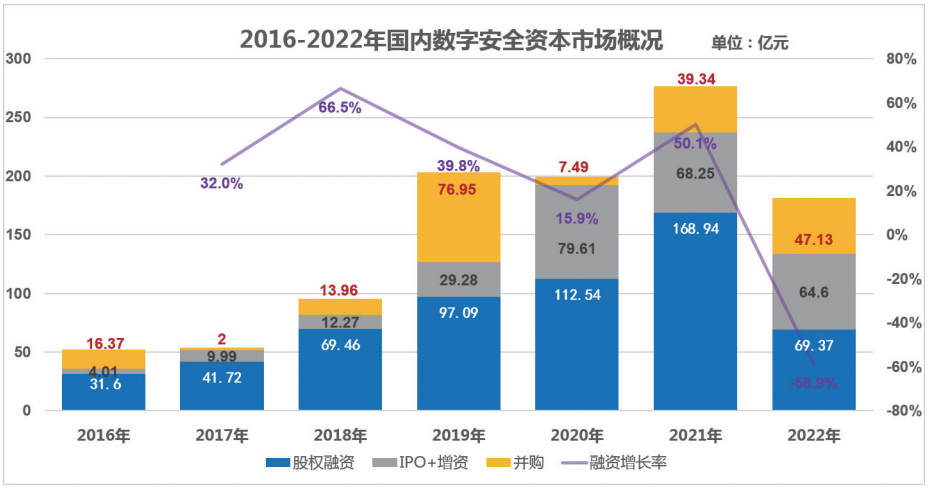


图 43　2016-2022 年国内数字安全资本市场概况

在融资热点方面，与 2021 年度相比有了一些变化。隐私计算、安全运营和身份安全暂时退出，攻击面管理、车联网安全跻身，而云原生安全开始与业务安全（API 安全）结合。

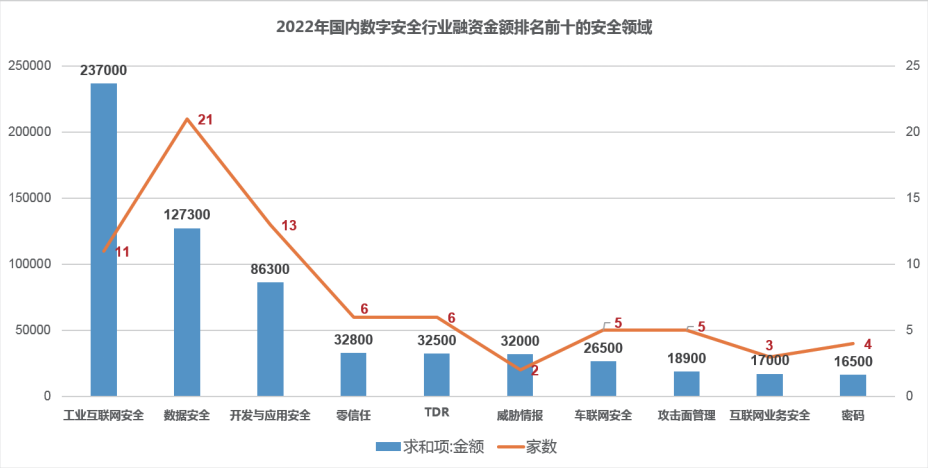


图 44　2022 年国内数字安全行业融资金额排名前十的安全领域

重要结论

●2016 年至 2022 年，国内数字安全资本市场，累计股权融资总额超过 590 亿元。

●2022 年融资市场大幅度下滑的原因，除了三年疫情、国与国争端以及全球经济疲软的大背景之外，数字安全企业的规模扩张和净利润增长始终处于困境，投资回报率普遍偏低，因此投资界对整个产业的良好预期缺乏信心。

●“长持有、多赛道、共成长”是数世咨询于 2021 年提出的投资理念，基于这一理念来看，主要依靠融资扩大规模以占领市场，之后再设法回归企业良性发展的互联网模式并不适用。

第六章　数字安全九大态势

2023 年，对于数字安全产业的大多数民营企业来说，生存是第一要务。对于整体数字安全产业而言，长期向好，未来可期！

——数世咨询

一、数字安全时代的到来

数世咨询认为，计算机安全、信息安全和网络安全三个时代，可由《中华人民共和国计算机信息系统安全保护条例》、《国家信息化领导小组关于加强信息安全保障工作的意见》，和“没有网络安全，就没有国家安全”等国家层面的法规政策和方向指引来划分。而中共中央、国务院印发的《数字中国建设整体布局规划》，则标志着 2023 年是数字安全时代的开启元年。

二、国有化趋势愈加明显

安全是一个特殊的领域，机构主体规模越大就越无法做到独善其身，其自身的安全与否直接或间接影响到社会和公共安全，政治和国家安全。只要是事关国计民生的重要领域，就需要从更高的维度来管理和把握。基于这个底层逻辑，未来会见到更多的国资入股或收购民营安全企业。同样也基于这个逻辑，也解释了大型国有企业纷纷成立数科公司，即“数科化”的原因。

“未来绝大多数大型数字安全企业都将或多或少的具备国资身份。”--摘自数世咨询《中国数字安全产业统计与分析报告（2022）》

三、集成模式挤压利润与创新空间

安全的特殊性决定了国有化的趋势，但同时也带来了数科化，加重了数字安全市场上集成模式的比重。正如报告上文的统计，2022 年度数字安全市场仅有的 7% 增长，全部来自集成业务。集成的好处在于，为供需双方提供缓冲区，具有政治与经济利益的双重保证等内在价值。但同时，也存在着明显的弊端，即严重挤压原厂商的利润空间，安全企业疲于生存，创新就无从谈起。

四、数字安全产业发展形势严峻

自数世咨询核心团队开始产业统计工作以来，这是首次公开表示对产业发

展形势的担忧。数字安全市场规模的增速和利润，已经连续二年急速下滑，而且势头难止，很大程度上意味着今年产业规模的停滞，甚至是倒退。对于大多数民营企业而言“生存是第一要务”，尤其是严重依赖融资输血的企业，面临的是生死存亡问题。而对于当下想要创业的人来说，则是“市场有风险，创业需谨慎。”

五、国家安全、数字经济为刚需

数字安全产业的两大核心驱动力，一是国家安全，二是数字经济。两者互为依赖、互为因果。“以新安全格局保障新发展格局，要坚持发展和安全并重，以安全保发展、以发展促安全”。近两年来由于政治、经济、疫情等内外环境的各种因素影响，产业出现连续下滑的态势，但数字安全产业的刚需是国家安全，是数字经济。因此，虽然出现暂时的疲软停滞，但“长期向好，未来可期”的大趋势不变。

六、存量市场与增量市场并发

国内用户的数字安全能力或需求呈阶梯状。从拥有丰足的安全预算投入、成体系的安全产品和豪华安全团队的超级用户，到具备基础安全能力水平的一般用户，再到缺人少钱的用户，甚至还有无预算、无工具、无人员的“三无用户”。究其原因，中国各地区、各行业、各组织的经济发展水平差异较大，信息化、数字化程度也参差不齐，数字安全的能力或需求自然也是高低不等。这种阶梯状，意味着国内不仅有对传统安全合规产品的大量需求，即存量客户，主要集中在政府部委和央国企，还会有数字经济驱动下的创新安全产品的广阔发展空间，即增量市场的需求。数字安全行业的未来，将会是合规与创新的双轮驱动。

七、一体化解决方案呼声渐强

非常注重数字安全体系化建设的用户，以及面临庞杂的数字化运营工作的用户，开始出现摆脱安全产品的“最佳选择”，转向产品和供应商整合的倾向。

因此，集成多种具备某种共性产品的安全平台，即基于平台的一体化解决方案，越来越受到供需双方的高度关注。如云原生应用保护平台 CNAPP、安全可见性 / 优先级和验证的 SOPV、扩展检测和响应 XDR、零信任访问架构 ZTNA、安全访问服务边缘 SASE，以及数世咨询提出的持续应用安全 CAS、数据访问安全域 DASS、一体化端点安全 IES、安全驱动的数据治理 SDDG 等。但由于商业壁垒和体制文化等原因，融合类的一体化解决方案供应侧能力严重不足，往往最终的采购结果会变成总包性质的大集成模式。

八、安全运营从共识走向落地

安全的动态性、伴生性、系统性和服务性，要求必须引入运营的理念。用户真正需要的是安全能力、安全效果的提升，而不是安全设备、软件等产品的堆砌。在前几年，业界已经取得了安全运营理念的共识。现如今，具备一定数字化水平并拥有独立安全团队的用户，普遍的在开展安全运营工作。一些前瞻性的客户，甚至开始尝试接受远程安全托管运营的模式。根据对甲乙双方实际情况的调研和总结，数世咨询提出安全运营的五要素：工具、人、平台、流程和管理。

九、数据安全新方向逐渐明朗

2022 年底，《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”），为解决数据要素化最大的难点 -- 数据确权，创造性提出了“淡化所有权、强调使用权，聚焦数据使用权流通”的“三权分置”数据产权制度框架，提供了突破数据确权困境的可能，并“鼓励探索数据流通安全保障技术、标准、方案”。数世咨询认为，未来三到五年的主流数据安全需求，将聚焦在“数据主体可控的有限范围内，即机构内各部门、合作伙伴、供应商、用户”的数据访问场景上。

后 序

将产业统计分析报告做的真实客观，是一件非常耗费人员、时间和精力的复杂性工作。考虑到商业价值的话，并非一件“划算”的事。但一份能够真实反映客观现状的年度报告，无论是对产业的布局规划，还是对技术的趋势判断，亦或是对创业者、投资人的方向指南，都是极具价值的重要参考资料。尤其是对已经在产业方面有着多年经验积累，并掌握实际工作方法的调研机构而言，更是一件责无旁贷的工作。

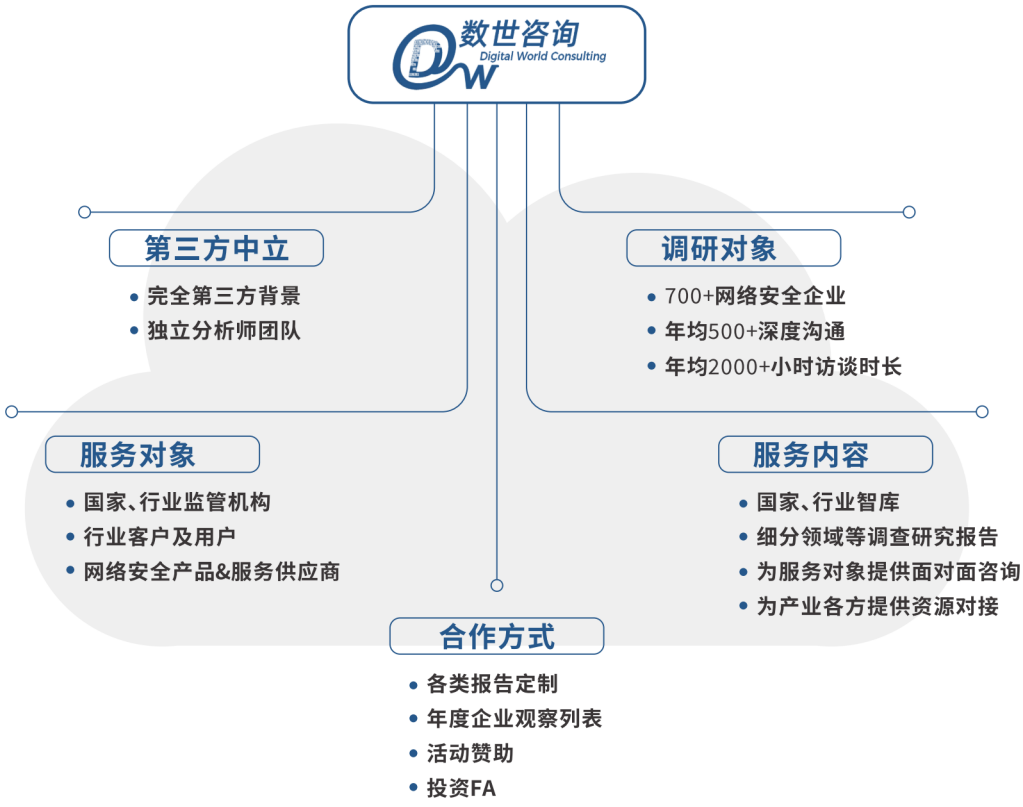
但如何将产业年度报告做的真实客观？如果仅靠网上搜集资料，找几个业内人士做个访谈，再发个调查表让大家填一填，然后坐在电脑前用公式推导计算，这样的报告肯定水分很大，但的确是一大批报告撰写者的常态。

质量高的报告如何做？说出来可能会令人嗤鼻，因为使用的方法也无非上述的发表、访谈和搜集，但区别在于实操。调查表中填写的数据和真实数据是不一样的，访谈几位业内专家和访谈几百位企业经营者是大不一样的。做好调研工作，其实一句话足矣：

没有调查就没有发言权。

在完成整篇报告的撰写工作之后，看看飞书里拥挤的日程表，意味着数世咨询分析师团队接触过的几百家厂商，访谈过的千余位销售、解决方案、产品经理、创始人……虽然辛苦但成就感满满，信息量满满。

“摸清家底”，了解现状、提出问题，才能做出合理的规划，辅助高层决策，以更好的解决问题，这是数字领域每一家调研机构的立身之本，也是职责和使命。数世咨询将会同广大业界同仁，不断的将调研工作补充完善，为产业发展、技术进步和战略决策提供有力支撑，为国家安全的保障、为数字经济的发展，贡献自己的力量。



北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业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，撰写发布过《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》、《中国数字安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、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 700 余家，以及 150 余家有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，投融资对接，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：北京市东城区鲜鱼口街 90-2 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

数字安全领域中立第三方调研机构