数据安全推进计划
DATA SECURITY INITIATIVE

数据安全产品与服务观察报告

版权声明

免责声明

数据安全推进计划取得数据的途径为公开资料、厂商调研与行业访谈。本报告力求内容客观公正，但所载观点及其他数据信息仅供参考使用，对依据或使用本报告所造成的一切后果，本报告及作者不承担法律责任。

前　言

2023年，中共中央、国务院印发《数字中国建设整体布局规划》（以下简称《规划》）。《规划》强调要推进数字技术与经济、政治、文化、社会、生态文明建设“五位一体”深度融合，强化数字技术创新体系和数字安全屏障“两大能力”，　由此可见技术发展在数字产业规划与数字经济发展中的重要作用。

数据安全作为发展数字经济的能力底座，其技术产品及服务能力备受关注：

数据安全技术是数据安全厂商立足之本。数据安全技术以数据为核心，围绕数据在全生命周期中的安全需求，通过对数据的识别、标记、变形、计算等操作，保护数据的持续安全状态。数据安全厂商通过组合、应用一种或多种数据安全技术，形成丰富的数据安全产品及服务，实现数据识别、检测、防护、监测、隐私保护、追踪溯源等场景下的目标。随着各行业组织的数字化转型持续深入，数据安全事件频发，数据安全风险严重，业内多方亟需支持数据安全产品及服务厂商通过技术创新与应用，持续提升数据安全能力水平，发展壮大我国数据安全产业。

产品与服务的持续创新是数据安全厂商发展之阶。近几年，我国数据安全产业发展迅速。为深化调研我国数据安全产品与服务市场现状，2022年，数据安全推进计划面向116家数据安全产品、服务供应商，开展两轮数据安全产品与服务调研，将数据安全产品与服务分为数据资产识别类产品、数据安全检查类产品、数据安全防护类产品、数据风险监测类产品、数据共享流通安全类产品、数据安全合规类服务、数据安全能力提升类服务等品类板块，合计调研488款产品及服务，并形成《数据安全产品与服务图谱2.0》（以下简称“图谱”）。

本报告基于图谱数据，对我国数据安全产品、服务、市场的现状进行介绍、分析，形成数据安全产品与服务的十大观察观点。

特别鸣谢机构

中国信息通信研究院云计算与大数据研究所、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、联通数字科技有限公司、杭州美创科技股份有限公司、北京安华金和科技有限公司、全知科技（杭州）有限责任公司、杭州极盾数字科技有限公司、深圳昂楷科技有限公司、北京亿赛通科技发展有限责任公司、数安信（北京）科技有限公司、杭州薮猫科技有限公司、江苏保旺达软件技术有限公司、北京奇虎科技有限公司、中国电子科技网络信息安全有限公司、北京数字认证股份有限公司、神州融安数字科技（北京）有限公司、深圳市洞见智慧科技有限公司、天道金科股份有限公司、安徽辰图大数据科技有限公司、天翼安全科技有限公司、杭州雅拓信息技术有限公司、南京聚铭网络科技有限公司、厦门服云信息科技有限公司、杭州金智塔科技有限公司、杭州比智科技有限公司、北京炼石网络技术有限公司、北京数安行科技有限公司、苏州美天网络科技有限公司、深圳市华傲数据技术有限公司、新华三技术有限公司、中兴通讯股份有限公司、中电科拟态技术有限公司、深圳市联软科技股份有限公司、浙江泽大律师事务所、浙江寰福科技有限公司、上海观安信息技术股份有限公司、科大讯飞股份有限公司、深圳红途科技有限公司。

特别鸣谢专家

龚诗然、李天阳、张越、林鹭、程文博、楚赟、赵宁、崔玲龙、王英杰、薛恺、李阳、谭峻楠、周顿科、查浩奇、李方方、赵汝东、乐凯明、黄哲慧、李楷、张艺伟、梁晓云、胡国华、张红露、孟晨、傅娅兰、刘险峰、钱戈、卢伟、唐会芳、薛锋、王晗、王翀、李登峰、宁立君、王皓、李博、李绍宾、韩晓宇、王同新、关中华、项宇欣、张鑫、陈韬、陈虎、余志军、杨智垄、陈超超、梁腾文、何夕、曾博、薛诗静、赵倩、刘玉红、曹峰、何旭珩、王曦光、王文娟、侯大鹏、耿蕴秋、杨学治、高云翔、孙权、甘铜、谢江、包宏宇、倪修峰、杨培、王慧敏、黄俊辉、陈冰洵。

目 录

一. 数据安全产品与服务发展概述 1

(一) 数据安全产品 1

(二) 数据安全服务 5

二. 数据安全产品与服务观察 9

(一) 智能化浪潮来临:数据安全产品技术升级 9

(二) 新技术:深刻影响数据安全产品发展 10

(三) 第三方评测:“以评促建”创造厂商新优势 14

(四) 安全检查工具:供给难以满足市场需求 15

(五) 数据防泄露:安全防护领域的重点产品 17

(六) 数据安全网关:产品形态缺乏统一共识 19

(七) 数据风险监测:站在“一体化”的“分岔路口” 22

(八) 运营管理平台:“平台化”趋势下的热门产品 23

(九) 安全合规服务:咨询与评估成为业内焦点 25

(十) 分类分级服务:逐渐演变为独立服务品类 27

附录 30

(一) 综合型厂商 31

(二) 专业型厂商 46

(三) 新兴型厂商 60

图目录

图1 图谱:数据安全产品与服务图谱框架 2
图2 数据安全产品分布 2
图3 图谱:数据安全防护类产品 3
图4 图谱:数据安全服务 6
图5 数据安全服务分布 6
图6 数据安全厂商分布 8
图7 图谱:隐私计算产品 11
图8 厂商第三方评测与平均单年营收统计 15
图9 图谱:数据安全检查类工具 16
图10 图谱:数据安全网关产品 21
图11 图谱:数据安全运营管理平台产品 23
图12 图谱:数据分类分级服务 28
图13 奇安信数据安全产品布局 32
图14 奇安信数据安全服务框架 33
图15 奇安信数据安全服务流程 33
图16 奇安信数据分类分级服务流程 35
图17 亿赛通数据安全产品布局 37
图18 亿赛通数据安全服务案例 39
图19 保旺达数据安全产品布局 40
图20-1保旺达数据安全产品架构(数据资产梳理系统) 41
图20-2保旺达数据安全产品架构(接口安全管控系统) 42
图20-3保旺达数据安全产品架构(文档安全流转中心) 43
图21 保旺达数据安全服务案例 45

图目录

图22 安恒信息数据安全产品布局 47
图23 安恒信息数据安全服务框架 48
图24 安恒信息数据安全细项服务简介 48
图25 美创科技数据安全产品能力全景图 50
图26 美创科技数据安全咨询服务体系 52
图27 美创科技数据安全运维服务体系 53
图28 美创科技数据安全运营服务体系 53
图29 炼石网络数据安全产品矩阵简介 55
图30 炼石网络数据安全服务框架 56
图32 数安信数据合规管理能力体系 58
图33 数安信数据安全合规服务框架 59
图34 数安信数据安全服务案例 59
图35 融安数科隐私计算引擎产品架构 61
图36 融安数科隐私计算解决方案架构图 62
图37 洞见科技InsightOne平台相关场景解决方案 64
图38 洞见科技精准投放场景解决方案 65
图39 洞见科技数据要素安全交易场景解决方案 66
图40 金智塔科技“智隐隐私计算平台”架构图 68
图41 金智塔科技“智通数据要素流通平台”架构图 69
图42 金智塔科技统计数据合规应用场景解决方案 70
图43 金智塔科技小微企业授信融资场景解决方案 70
图44 金智塔科技政务数据融合场景解决方案 71

一、数据安全产品与服务发展概述

组织的数据安全建设理念转变带来产品、服务的变化创新。相较于传统网络安全基于系统的安全防护，数据安全从业务需求出发，强调覆盖数据全生命周期的技术、产品与能力布局，重点关注何种数据、分布何处、如何流转、谁在使用、如何防护等关键问题。

本报告根据数据安全产品的安全能力、面向的数据形态等多个维度，将数据安全产品分为数据资产识别、数据安全检查、数据安全防护、数据风险监测、数据共享流通安全等领域，形成兼顾安全与合规、覆盖“识别-检测-防护监测”的产品布局。而数据安全服务则根据服务需求方的目标与期望，分为合规类服务与能力提升类服务。

（一）数据安全产品

以数据为中心的安全防御体系逐步建立。根据图谱，数据安全产品的应用贯穿数据的全生命周期：无论是数据采集阶段的识别、标记、分类分级，还是存储、使用阶段的加密、脱敏、审计，以及共享流通阶段的隐私计算、数据水印等产品工具，均为保障数据的保密性、完整性、可用性，以及数据处理活动的合规性、可控性提供了技术支撑。

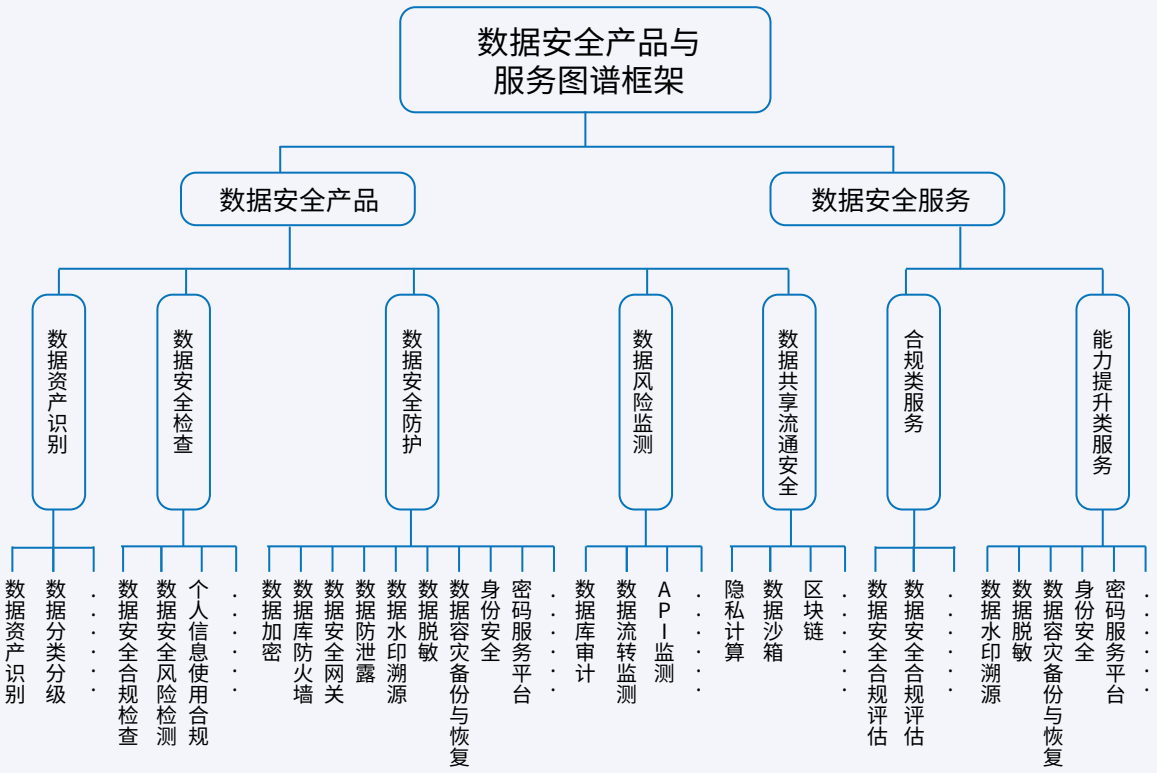


图1 图谱：数据安全产品与服务图谱框架

数据安全产品广泛应用于在数据资产识别、数据安全检查、数据安全防护、数据风险监测、数据共享流通安全，整体上呈现出多层面、全方位的数据安全理念。然而，从产品数量的分布上看，数据安全防护类产品数量占数据安全产品总数的43%，呈现出目前以“防”为主的安全理念。

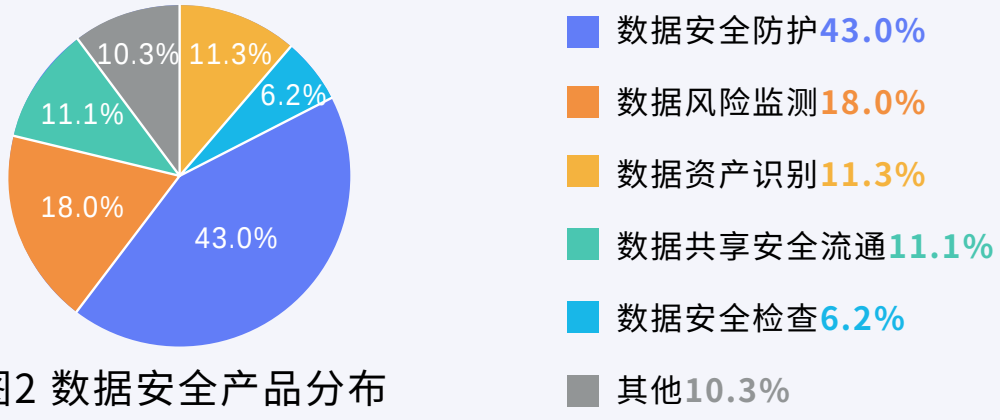


图2 数据安全产品分布

图3 图谱：数据安全防护类产品

1.数据资产识别

数据资产识别类产品包括数据资产识别、数据分类分级等产品，主要应用于组织发现、识别、管理数据资产，覆盖了结构化数据与非结构化数据。数据资产识别产品主要通过自动化识别技术（例如：文本识别、图片识别、关键字匹配、正则表达式匹配等），基于识别规则对组织的数据源进行全面扫描、筛选、梳理、分析，帮助组织识别、发现数据资产类型和量级，全面盘点组织内部的数据资产。数据分类分级产品则在此基础上，通过数据自动发现技术，基于产品内置的规则对组织的数据进行识别、分类、分级，形成可视化、可输出的分类分级成果，从而实现差异化、精细化的安全保护与管理。

2.数据安全检查

数据安全检查类产品主要包括数据安全合规检查工具与数据风险检测工具。数据安全合规检查工具基于数据安全相关法律法规要求，对数据脱敏、违规采集、数据销毁等安全控制措施的有效性进行检测，判断数据安全现状与测评指标的符合程度。数据风险检测工具则主要通过流量分析等方式，盘点敏感数据暴露面与流动情况，开展漏洞及配置检测，识别包括账号、权限、暴露面、行为在内的诸多数据安全风险要素。

3.数据安全防护

数据安全防护类产品涵盖了数据保护类、访问控制类、追踪溯源类的诸多产品。数据安全防护类产品以数据为核心，围绕全生命周期进行防护，依托加密、脱敏、身份认证、访问控制、监控审计等技术，贯穿数据、终端、应用、系统、网络、物理等层面的安全技术及工具部署，实现多方式、多层次的产品技术互补，提升终端数据安全、网络数据安全、平台数据安全和应用数据安全的防护能力，实现安全可信、安全可管、安全可控。

4.数据风险监测

数据风险监测类产品主要包括数据库访问监测、API安全监测、应用访问监测等产品，主要提供聚合态势呈现、风险预警、安全运营、威胁分析、事件溯源等风险监测能力，实现对组织数据处理活动的风险实时动态监测。此外，随着各行业数字化转型进程加快，单点工具的简单堆砌已无法满足组织面临的复杂数据安全风险，亟需引入一体化的监测类产品，形成“以点

向面”的产品布局与能力支撑，通过规范化、集中化的数据安全管控策略管理，提供组织数据安全运营、运维、风险监测、事件管理管理等功能。

5.数据共享流通安全

随着数据要素市场化步伐加快,数据共享流通安全类产品基于隐私计算、区块链等新兴技术，与其他数据安全技术进行协同与融合,助推数据要素安全流通,推动数据要素合理化配置,进一步释放数据价值。在满足数据隐私保护与数据流通融合需求的整体目标下，数据共享流通安全类产品将难以共享的数据通过隐私计算等技术应用，促进数据要素跨域流通和应用的安全合规。

(二) 数据安全服务

数据安全服务种类增加，服务内容持续完善。相对于传统网络安全服务往往仅作网络安全技术产品的“附属品”，由于数据作为新型生产要素与业务耦合度深、流转范围广的特点，数据安全服务种类更加多样，也更重视服务内容多样性与服务的品质。

数据安全服务指数据安全服务的提供方使用其自身资源来支持数据安全服务需求方对数据安全管理的服务提供。数据安全服务可以分为合规类服务与能力提升类服务，合规类服务包括合规评估、合规咨询，能力提升类服务则包括管理体系建设、数据分类分级以及数据安全运维、人员培训、应急演练、数据安全保险等。

图4 图谱：数据安全服务

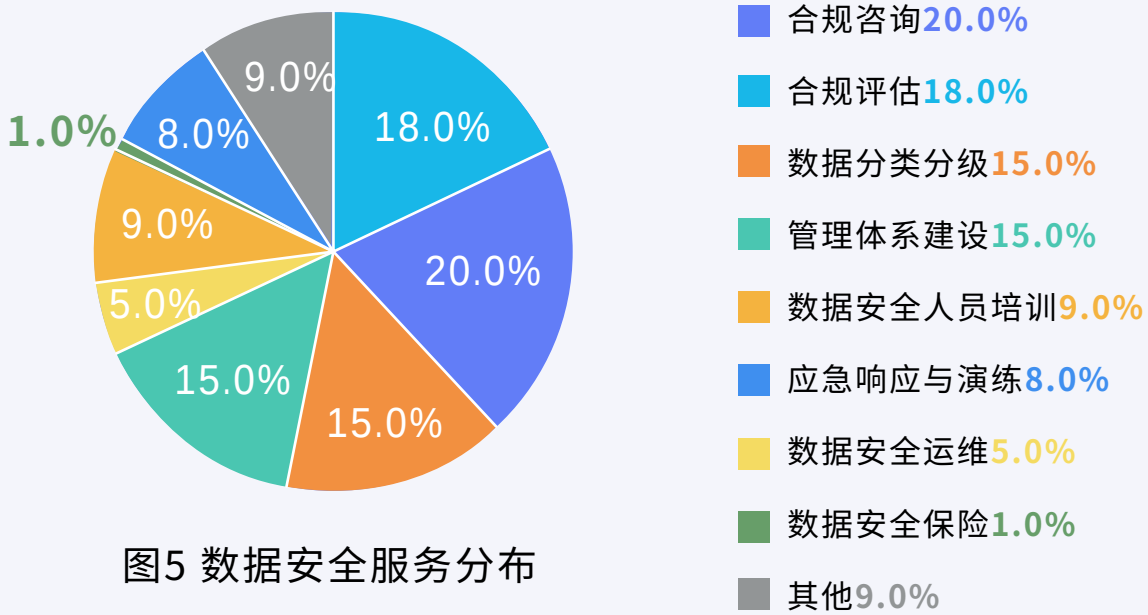


图5 数据安全服务分布

此外，在本次对于数据安全产品与服务的调研中，发现目前数据安全产品与服务机构的分布仍呈现碎片化的特点，在地域、行业等维度的集中度不高。根据对厂商的采访调研，参考参与图谱调研的116家机构近三年内的经营信息、营收表现、数据安全产品及服务数量、行业用户客户案例、第三方评测等方面信息，将数据安全厂商分为综合型（32.8%）、专业型（37.9%）、新兴型（16.4%）。

综合型厂商（32.8%）通常是早期（2019年以前）依托业务沉淀大量安全技术及应用经验的ICT、大型互联网公司或头部网络安全厂商。其中，个别厂商机构单年业务营收已达到十亿级。近几年，这类机构的业务重心逐渐移向数据安全领域，但相对于其整体营收，数据安全业务的营收、投入在整体业务规模中占比较小。综合型机构的数据安全产品相对全面，基本全面覆盖了数据识别、检测、防护、监测等方向，且通常在单个方向具备多款产品，整体产品布局呈现出“遍地开花，综合发展”的态势。从产品数量上看，大部分综合型机构的产品布局侧重于数据安全防护方向，体现了以“防”为主的安全理念。综合型机构基于前期在网络边界安全领域的实战沉淀与项目经验，在行业头部客户或大型安全项目的竞争中具备较强的优势，现已具备成熟的解决方案与服务能力。

专业型厂商（37.9%）主要是早期（2019年以前）依托数据库、数据库安全业务发展的头部厂商，部分厂商机构已入选“专精特新”组织。厂商机构在数据库安全领域具备丰富的积累与沉淀，数据安全业务已成为厂商机构的主营业务，大部分厂商的拳头产品包括数据库安全审计、数据防泄露、数据库加密等安全监测、防护类产品，目前随着数据的高频使用与流转，厂商

机构的产品重心也从数据库走向基于数据的全生命周期安全，并已在业内推出高知名度的数据安全建设经验或理念，并据此形成一系列的解决方案。

新兴型厂商（16.4%）主要是近年基于特定的新兴技术（例如：隐私计算、人工智能等）发展数据流通安全相关业务的初创厂商。随着国家法规政策提出“建立健全数据流通管理体制机制”，助力数据价值的安全释放。在政策与需求的双重推动下，大型互联网公司、厂商机构等均逐步开展隐私计算、智能数据运营等领域相关产品、技术布局，市场格局逐渐稳定。从产品数量上来看，厂商机构专精于某一至两个方向，主攻隐私计算、多方计算等方向，赛道内的头部厂商已占领大部分市场份额，持续打造细分赛道的纵深竞争力，目前备受投融资市场青睐。相关产品也从落地初期验证阶段进入加速落地阶段，但部分产品的同质化趋势明显。

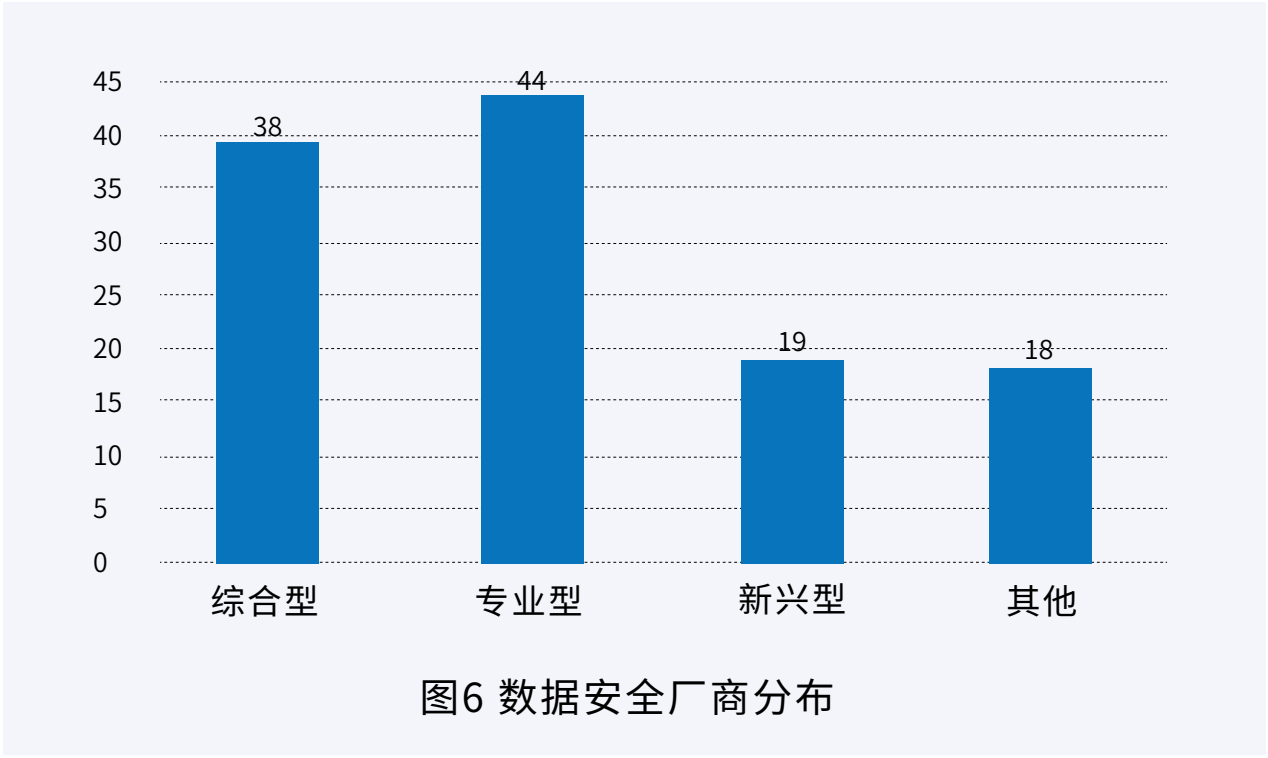


图6 数据安全厂商分布

二. 数据安全产品与服务观察

本报告基于图谱调研信息与业内专家访谈、研讨结论，从不同的数据安全产品与服务入手，分析产品发现现状与技术发展理解，阐述典型产品的发展问题、技术优劣势与未来趋势，形成以下十项观察，为组织的数据安全体系建设提供产品与技术参考。

(一) 智能化浪潮来临：数据安全产品技术升级

人工智能赋能数据安全。2023年，微软提出“AI安全副驾驶”，认为人工智能能够利用安全模型收集有关潜在威胁，追踪网络攻击风险。人工智能通过获取、收集和分析更多用户和组织数据，提升和优化语义分析、内容理解等方面技术能力，能够对收集的海量数据进行快速分析和分类管理，实现数据安全产品在效率、精细度上的显著提升，并一定程度上降低检索与筛选的时间成本，极大地释放人力。

人工智能技术的应用反映了从静到动的安全防护策略转变。数据安全风险与组织业务发展休戚相关，组织业务的持续运营离不开对数据安全风险的实时管控，因此静态的风险管理规则已不适应难以满足当前对于数据安全风险的动态防护需求。人工智能技术通过实时学习能力，驱动数据安全治理向智能化、高效化、精准化方向演进。

提升数据分类分级产品技术的准确性及工作效能。组织多源异构的海量数据嵌套于复杂的业务场景中，为数据分类分级带来巨大挑战，亟需依托自动化的产品工具保障分类分级工作的高效、准确。这也直接推动了数据分类分级产品的技术创新：图谱数据显示，35.3%厂商向组织提供自动

化、智能化的数据分类分级工具，部分厂商将数据分类分级产品与机器学习算法规则相结合，利用人工智能技术对复杂的上下文进行分析，生成敏感数据分布，便于用户掌握敏感数据类别以及使用情况等信息，并通过机器学习、自然语言处理、图像识别等技术对数据资产进行梳理，形成标注样本，并通过持续训练提升数据分类分级效率。

提升数据安全风险监测技术的自动化响应能力。人工智能的自动学习能力能够从海量数据及行为中识别恶意程序以及其他欺诈行为，实现对数据安全的智能化监测防护，对引起数据态势发生变化的安全要素进行“获取、理解、显示”，其自主决策能力能够通过发掘数据处理日志，检测攻击者的行为特征并加以拦截，结合威胁情报以及预判的未来趋势，实现对数据风险事件的自动化响应，避免组织服务和数据被破坏。

在人工智能引起新一轮技术变革的同时，我们也应正视人工智能技术应用带来的全新的数据安全威胁。2022年ChatGPT横空出世，其依托强大的基础模型、高质量的样本数据、基于人类反馈的强化学习这三项关键能力，极大地降低了攻击行为的技术门槛——这对数据安全产品乃至全行业带来极大的影响和冲击，可以预见未来在模型的建立、训练过程中，以数据污染、数据泄露、数据滥用为代表的数据安全威胁将导致安全攻防态势愈发激烈，这也对数据安全厂商及产品带来更大的挑战与考验。

(二)新技术：深刻影响数据安全产品发展

1.隐私计算

隐私计算为数据安全合规流通提供技术支撑。如今隐私泄露已成为不容小觑的数据安全威胁。隐私计算技术能够在不泄露原始数据的情况下，

安全地加密、处理、计算数据，能够有效应对数据在流通应用过程中面临的泄露风险，进一步挖掘数据价值。

隐私计算技术产品落地应用逐渐广泛。2023年1月发布的《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》中提出，加强隐私计算技术攻关和产品研发，在政策红利和安全需求的双重驱动下，隐私计算技术与产品已从落地初期验证阶段进入加速落地阶段，现已广泛应用于政务、金融、通信、医疗、互联网等行业，在公共数据开放、智能营销、联合风控等行业典型场景下持续落地。目前多地政府、中大型银行、运营商、医疗机构等均着力建设隐私计算平台。

图7 图谱：隐私计算产品

尽管隐私计算产品一定程度上解决了数据使用过程中的安全问题，实现了“数据可用不可见”，但**隐私计算产品在规模化应用过程中面临三大挑战：一是安全与性能平衡有待探讨。**隐私计算依托复杂算法保障安全，然而算法的复杂度将直接影响计算效率，安全与性能之间的平衡是隐私计算产品应用面临的一大挑战。**二是通用解决方案难以应对复杂场景。**受多参与方、高时效性要求、复杂应用模式等客观条件影响，且不同的数据使用共享场景差异大，通用的隐私计算产品难以直接适配场景需求，应用门槛与成本较高。**三是互联互通面临阻碍。**市面上的隐私计算产品在框架、协议以及

底层技术方面存在差异，产品存在互联互通障碍，用户应用过程中也易出现重复投资风险、系统资源冗余消耗和产品选型受限等问题，亟需基于统一的标准强化产品的互联互通能力。

然而，以上问题无法单纯依靠厂商技术迭代解决，未来亟需产业多方合力攻克，实现隐私计算产品在效率、成本、互联互通方面的持续改进。**一是多技术路线融合。**通过隐私计算自身多技术路线融合，以及与人工智能、区块链、Web3.0等新兴技术融合应用，打破技术瓶颈，持续实现计算效率与安全性、互联互通性等方面的平衡。**二是持续控制产品运营成本。**隐私计算产品应用提供更“普惠”的产品应用门槛与安全能力，通过高度集成化、计算模型标准化、可视化等方式持续控制产品运营成本，提升用户使用体验、产品便利性。**三是互联互通进程将显著加快。**目前中国信息通信研究院联合多家主流隐私计算厂商建立“隐私计算联盟互联互通推进计划”，逐步探索异构隐私计算平台间的互联互通，厂商之间已从散点联合、验证探索的阶段逐渐迈进“织点成网”、协同推进的新阶段。这也意味着未来业内将出现更多的完整、成熟的互联互通落地方案，持续构建多行业、多领域的可信数据流通生态。

2.量子计算

量子计算技术的出现将对当前广泛使用的基于公钥密码体系的加密算法构成安全威胁：量子计算机具备在短时间内破解大规模的基于公钥密码的加密算法的能力。这意味着依托于传统加密方法的数据安全产品需要更强大的加密机制保障敏感数据的机密性，以应对日益严峻的攻击勒索态势。

量子加密技术为此提供了可能。量子加密技术基于量子力学原理，利

用量子态的性质进行加密和解密。量子加密技术的实现需要量子密钥分发（QKD）协议，该协议利用量子比特之间的相互作用来分发密钥。由于量子态的测量会改变它的状态，所以任何第三方的窃听或干扰都会被检测到。这意味着量子加密能够为数据安全产品提供更高强度的加密处理能力，并持续提供高性能的并发处理支撑，大幅提高密码分析、模式识别和人工智能等方面的计算能力，即使是量子计算机也无法破解。

随着量子计算的发展以及商用化，未来量子加密技术或将成为数据安全产品中的必要组成部分。然而，量子计算机的构建、操作需要可靠的量子通信基础设施（包括光纤、量子中继器、量子存储器等硬件支撑以及针对量子计算的专用算法等），且技术应用成本高，目前在实际应用过程中仍面临落地挑战。此外，为确保其在不同系统、应用之间的兼容性与互操作性，量子加密技术应用也亟需业内加速制定相关标准，以满足不同行业、领域、场景的需求，实现更可靠、高效的量子技术应用。

3.区块链

区块链成为可信数据基础设施的关键一环。随着“数据要素化”趋势渐显，各类组织对自身数据的流通提出了更高的安全要求。区块链通过形成安全、连续、不可篡改的链式数据结构，使其在数据权属主体确认、数据流通追踪溯源、多主体数据共享管理等方面发挥重要作用。依托这种新型的信任服务基础设施，区块链在数据防篡改、可溯源取证等相关场景（例如：主体确认、追踪溯源、数据安全事件审计与追责等）能够为数据权属的主体确认、数据流通的追踪溯源、数据变化的血缘关系等提供可信、安全的基础，以更加安全、自动化、机器化的形式为多方提供信任，一定程度上解决了数据在交换的过程中面临的所有权界定问题。

尽管区块链相关底层技术、插件发展逐渐成熟，目前技术应用与落地加速，市场需求持续攀升，但区块链自身存在的安全问题也逐渐显现（例如：合约代码漏洞等），面临效率与技术的双重挑战。此外，相较于传统的信用模式（例如：人治信用、权威信用、第三方公证等），由于区块链采用的是基于数学模型与密码学算法的机器信任模式，在实际应用落地阶段，区块链节点无法避免实体干预（个人、机构、组织等）。这也意味着如何最小程度避免人为因素扰动，保障数据在上链前与链下存储的安全可信，将是区块链与数据安全融合时亟需考虑的重要问题之一。

（三）第三方评测："以评促建"创造厂商新优势

"第三方评测"通常指专业机构通过评估、技术评测某一产品或横向对比同类产品的质量、功能、性能等方面情况，从而为用户提供专业、独立、客观的参考信息。第三方评测机构作为参与社会治理与市场监督的重要力量之一，在打破信息壁垒，助力供需适配的同时，也显著地影响用户的决策行为。

第三方评测助力厂商创造新优势。目前数据安全厂商积极参与数据安全产品评测：第三方评测在帮助厂商发现产品问题的同时，也为厂商提供向广大用户充分展示产品的优势与特色的途径。图谱数据显示，25.8%的厂商的厂商主动参与过数据安全产品与服务相关的评测，其中16.4%的厂商在近三年内实现过单年营收破亿。参与过评测的产品在招标项目中通常具备一定的优势，在厂商整体营收上普遍表现相对亮眼，且行业应用案例较多，逐渐演变为厂商的主打产品。

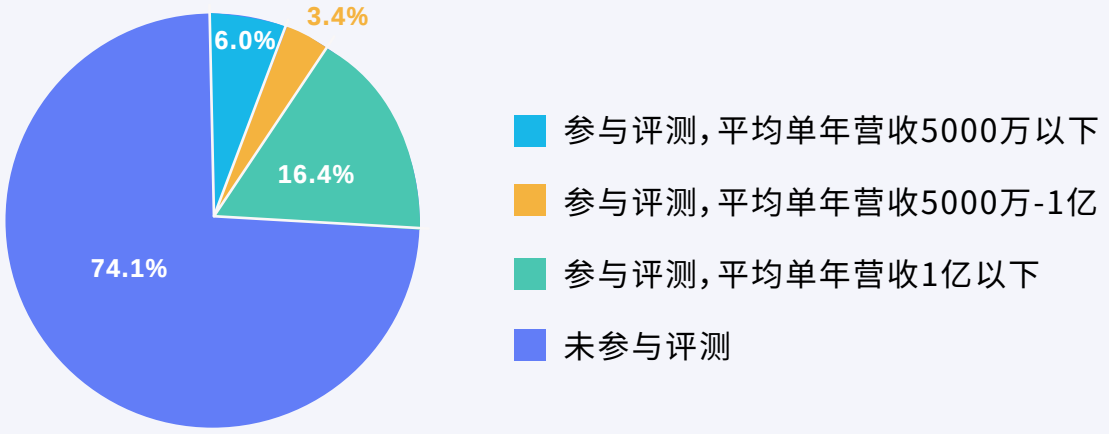


图8 厂商第三方评测与平均单年营收统计

第三方评测拉通对齐供需双侧认知。第三方评测能够一定程度上为需求侧组织解决对产品、服务以及厂商等服务机构本身的疑惑与担忧，推动服务机构持续完善产品、服务质量，从而助力培育良好的行业生态。未来，第三方评测机构在完善自身资质、保持独立性的同时，亟需面向数据安全产品、服务甚至厂商等服务机构建立评估评测体系，与参评厂商充分互动、发现问题并合力探讨解决良方，推动数据安全产品、技术、服务的高质量发展。此外，第三方评测机构还可通过信息公开平台、新闻等方式向业内用户公开评测成果，保障评测结果的充分应用，持续发挥第三方评测的价值。

（四）安全检查工具：供给难以满足市场需求

监管部门对数据安全的检查要求日益严格。在欧盟一般数据保护条例（GDPR）、美国加州消费者隐私法案（CCPA）为代表的个人数据保护法规的推动下，国外市场已逐步孵化了提供数据安全合规检测产品工具或技术服务的相关厂商（例如：Onetrust、Bigid等）。国内多部门、多角度、高密度的监管要求也使数据安全检查工具得到越来越多的行业用户关注，各行业主管

部门及监管部门正式承担数据安全管理、监管职责，组织作为数据处理者亟需开展数据安全评估检测工作，落实数据安全保护义务，数据安全检查工具的需求应运而生。

数据安全检查工具基于不同的检查目标与输入，数据安全检查工具主要分为合规检查与风险检测两类，这类产品主要通过提供预置、统一的检查标准，建立自动化的检测能力，提高监管机构或组织内部执行数据安全检查活动的效率。其中，合规检查工具主要应用于面向组织数据处理活动合规情况的检测，具体包括针对敏感数据的安全保障能力、数据处理主体的身份验证、访问控制以及数据处理活动的合规性；数据风险检测工具则主要应用于针对组织数据及数据载体的潜在威胁、脆弱性等风险要素的检测。

数据安全检查工具依赖明确的检查输入。受限于国内外监管合规体系庞杂、业内缺少可被工具直接识别、转化的数据安全检查标准，目前仅18.1%的厂商向组织提供数据安全检测工具，数据安全合规检查类工具仅在数据出境评估、APP隐私安全检测、个人信息合规使用等检查输入相对明确的场景下发挥有限的价值，数据安全风险检测类工具则主要在独立技术验证、上线安全检测等基于特定技术标准要求的场景下得以应用。

图9 图谱：数据安全检查类工具

数据安全检查工具在检查维度、精度上同样面临技术挑战。一是合规输入兼容挑战。各国、各行业的数据安全、个人信息保护要求不一致将严重影响工具输出结果的准确性、全面性，直接为数据安全合规检查带来阻碍。**二是大规模数据分析能力挑战。**数据安全风险检测贯穿数据及其他风险要素的识别、检测以及风险响应，这意味着检测工具需要快速分析、处理多类型、大规模的数据（包括网络流量、系统日志等），因此亟需引入人工智能技术，根据数据的上下文场景对其面临的安全风险进行识别与判断，提高检测的准确率与效率，提升工具对风险的检出能力、全面性。

未来，数据安全合规检查工具将基于更加明确的监管要求及通用的权威标准、技术规范持续完善、发展。数据安全风险检测工具则将持续向“实战化”方向发展，依托人工智能技术，全面识别技术、管理缺陷，持续提高风险检测与分析的精度。

（五）数据防泄露：安全防护领域的重点产品

IBM《2022年数据泄露成本报告》显示，2022年全球数据泄露平均成本高达435万美元，创下该年度报告17年以来的最高纪录，数据防泄露的重要性日益凸显。随着国际、国内监管要求趋严，数据防泄露产品市场需求持续走强：数据安全推进计划发布的《2022数据安全行业调研报告》数据显示，68.4%的组织部署了数据防泄露产品，数据防泄露产品已成为组织数据安全防护的重点产品。

相较于传统的安全工具通过限制数据访问或全网数据加密等方式防范数据泄露风险，数据防泄露产品依托产品的深度内容识别技术，结合加密、访问控制、审计等技术，兼顾数据的流动与安全，满足了组织多场景、精

细化、协同化的数据安全防护需求。此外，随着人工智能与机器学习的不断发展，数据防泄露产品在自动分类、标记敏感数据的同时，还将通过人工智能的多维风险建模匹配，实现对内部用户的行为和意图进行智能监控与预测，持续提升数据泄露监测与控制的速度、精度。

数据防泄露产品市场竞争激烈。数据防泄露产品市场需求旺盛，大量厂商均在数据防泄露产品及解决方案上积极布局：图谱数据显示，在数据安全防护产品领域，46.4%的厂商向组织提供数据防泄露产品及解决方案。数据防泄露产品数量超过30款，占数据安全防护类产品的22.5%。各家产品的核心技术与功能点基本一致，产品类型包括终端数据防泄露、网络数据防泄露、存储数据防泄露、应用程序数据防泄露等，广泛应用于金融、电信运营商、政务、医疗、工业等大多数行业领域组织。各类数据防泄露产品的主要应用能力如下：

（1）终端数据防泄露：关注终端层面的敏感数据发现与泄露防护。产品通过终端设备或服务端集中管控、虚拟化等部署方式，应用文件加解密、访问控制、脱敏、水印等关键技术，防范终端数据外发场景下的数据泄露风险；

（2）网络数据防泄露：关注网络传输过程中的敏感数据泄露防护。产品通过网络代理、网络出口旁路部署等方式，应用网络流量检测、防火墙、防入侵检测、防病毒、传输加密等关键技术，实现网络入侵、数据异常传输等场景下的数据泄露防护、审计；

（3）存储数据防泄露：关注存储数据的泄露防护。产品同样通过网络代理、网络出口旁路部署等方式，主要面向数据库、文件，通过应用加密、访问控制、脱敏、水印、审计等关键技术，解决数据库、文件数据及其备份数据面临的异常访问、使用等安全问题；

（4）应用数据防泄露：关注应用访问过程中的敏感数据泄露防护。产品通过网络代理、网络旁路部署、虚拟化部署等方式，基于大数据、深度识别技术，运用用户实体与行为分析（UEBA）、脱敏、水印等技术，重点防范应用访问过程中的数据泄露、篡改风险。

数据防泄露产品能力持续升级。随着组织数据的指数型增长及使用场景持续扩展、丰富，数据泄露的威胁变得复杂化和多样化，各行业、组织的的数据安全防护需求不同，数据防泄露产品在保障稳定高效的性能的基础上，持续适应复杂的业务场景，从单纯的工具演进成为综合的数据安全防护解决方案，向用户提供高兼容性、低使用成本的一体化解决方案——这也将成为数据防泄露产品的发展趋势之一：解决方案化。数据防泄露产品将发展为以数据资产为核心、异常行为检测为驱动、全网监控审计为保障的组织级解决方案。这些解决方案将贯穿组织数据的全生命周期，覆盖网络、邮件、数据库、移动应用、端点和内部业务应用的全IT架构，为用户提供更高的敏感数据资产可见性、更场景化的安全策略、更灵活的安全控制能力。

同时，如何充分满足多种环境下的泄露防护协同需求是数据防泄露产品面临的一大挑战：组织的数据使用场景日益复杂，涉及到包括端、网络、数据库、数据中台等在内的多种环境，数据防泄露产品呈现多种形态，在满足用户不同的需求的同时，保障数据防泄露产品在多种环境下的协同联动。

（六）数据安全网关：产品形态缺乏统一共识

传统安全设备难以应对数据访问、数据共享、数据运维等活动带来的安全挑战，用户迫切需要新产品实现细粒度的数据访问控制、数据审计，数据安全网关产品由此应运而生。数据安全网关通过建立统一的数据访问、

分发的出入口，访问多类型的数据源并发现敏感数据，对访问数据的用户身份、位置、行为等信息进行分析、处理，从而实现应用及数据的可信安全访问的“咽喉”作用。

数据安全网关与数据防泄露产品极易混淆。数据安全网关与数据防泄露两类产品由于防护对象均为组织的敏感数据，均将访问控制作为防护手段之一，故两类产品在应用过程中极易混淆。相较于数据防泄露产品，数据安全网关更接近“海关”：它能够查验、过滤“异常用户”与“用户异常（行为）”，识别、判断用户所携带的数据敏感程度、量级。这意味着数据安全网关产品应通过预设的访问控制策略防御面向数据的攻击操作或误操作行为，防范由此引发的数据破坏、数据泄露风险。

数据安全网关产品涵盖了面向数据提供细粒度访问控制及安全防护功能的一揽子产品。图谱数据显示，数据安全网关产品数量占安全防护类产品总数的13.2%。基于不同类型的访问协议、部署环境以及数据对象，数据安全网关可以包括内网接入网关、流量加密网关、数据库安全网关、应用数据安全网关等具体产品。这也正是数据安全网关产品间缺乏共识的首要原因：部署在何种层级（产品层、中间件层、网络层还是物理层）将直接影响数据安全网关所呈现出的产品形态。此外，造成数据安全网关产品形态缺乏共识的原因之二是由于各厂商的数据安全网关产品衔接了不同的安全策略（例如：水印、脱敏、加密、阻断、合规审批等），在具备了更差异化、多样化的安全能力的同时，其功能界限也逐渐模糊。

图10 图谱：数据安全网关产品

尽管在访问协议、部署位置、数据对象上存在差异，不同类型的数据安全网关产品仍应具备敏感资产（数据、业务）识别、身份鉴别与访问控制、异常行为识别与分析的核心能力。以数据库安全网关为例，数据库安全网关应具备数据库访问协议的识别与解析能力，能够实现访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级，且具备对面向数据库的恶意攻击行为进行识别与处置的能力。应用数据安全网关则通过解析http协议，应用敏感信息识别技术，记录应用及API接口的敏感数据流转日志，能够通过反向代理技术获取应用的流量或者特定行为、数据信息，应具备透明代理、流量管理、负载均衡、安全防护等方面的能力。

未来，数据安全网关产品将持续扩大数据对象范围（例如：支持更多的国际主流数据库、国产数据库与大数据组件），且由于协议、部署位置的差异性，数据安全网关产品还需要完善其兼容能力，通过提供“可插拔”的架构，实现业务、数据以及安全能力的快速接入，并持续控制性能损耗，避免对业务造成的访问性能下降、链路节点增加等风险。

(七) 数据风险监测：站在“一体化”的“分岔路口”

数据风险监测类产品提供持续安全保障。数据风险监测产品通过对数据流转过程中的应用、账号、API、数据库等关键要素进行全方位的监控与审计，全链路监测敏感数据的访问与使用情况，识别数据在流动各环节、场景面临的安全风险。图谱数据显示，数据风险监测类产品数量占数据安全产品总数的18%。

根据不同的监测对象，数据风险监测产品可分为数据库访问监测、API安全监测、应用访问监测、敏感数据流动测绘等，在组织持续监测数据的安全使用、流动中发挥了极大的作用与价值。同时，随着数据出境安全逐渐成为国家监管重点领域，针对数据出境场景的风险监测产品也应运而生。这类产品能够对组织的数据出境行为、流向等信息进行监测、分析，记录出境的个人信息或重要数据的类型与数据量，为组织开展数据出境安全风险监测提供技术支持。

相较于网络安全风险监测产品，数据风险监测产品的价值体现在其聚焦数据与数据流向，重点关注如何保障组织数据日常操作的安全性、数据向低安全域流动的场景下如何保障安全等问题，满足组织日益频繁、高速的数据流转下的安全需求。数据风险监测产品要实现对数据流转全链路的监测，需要其能够对数据流转过程中各个节点上的日志进行联合分析——这意味着产品需要具备对接多类型数据源的能力（包括终端、应用、数据库等），实现日志的统一管理、多源日志分析、告警归并处置，这也要求产品保障架构开放与处理性能稳定，从而实现对多源异构数据的分析处理。

未来，面对组织日益复杂的数据生态，数据风险监测产品的平台化、一

体化的趋势已逐渐明确：数据安全运营管理平台或将替代提供更为全面的风险监测能力，而数据风险监测领域的单点产品则作为大多数组织已具备的安全模块，也需要通过具备采集更多的网络安全设备、数据安全设备信息的能力，实现组织数据流转过程的全面、动态监测。这一点也有望通过业内补充、完善数据标准交换格式标准，规范产品协作的要求与标准，降低用户在应用不同厂商的数据风险监测产品时的联调工作量。

（八）运营管理平台："平台化"趋势下的热门产品

简单的工具堆砌易造成数据安全运营工作"断点"。目前组织具备大量的数据安全设备，《2022年数据安全行业调研报告》显示44%的组织已应用了五到八项相关的技术产品，19.3%的组织应用了超过八项以上的技术产品。然而，简单堆叠的产品应用将造成数据安全运营工作的"断点"，组织内部的安全产品、策略之间形成"能力孤岛"，最终导致数据安全运营效率低、成本高、成效小。

数据安全运营平台成为打破"孤岛"的关键。数据安全运营管理平台能够为用户提供统一的运营管理入口、全局一致的操作方式，实现对各安全工具的能力编排、调度。图谱数据显示，21.6%的厂商向组织提供以数据安全运营管理平台为代表的平台化产品，通过聚焦"人-业务-应用-数据"链路，打破单点能力边界，主要关注对外态势感知与对内业务免打扰，实现组织内部一体化的数据安全运营。

图11 图谱：数据安全运营管理平台产品

高业务耦合与持续运营是数据安全运营管理平台的核心价值点。数据安全运营与业务密不可分：为了降低安全运营成本，数据安全运营管理平台需要明确业务数据的发现、分级分类、数据认责、权限管控等标准，提炼多种业务模型，建立业务数据安全指标，并实现分析集中化、指标可视化、处置流程化，持续提升数据安全运营与业务运行的适配能力。这意味着数据安全运营管理平台实际接入的是组织的数据安全能力，而非简单的工具集成。因此，数据安全运营管理平台需要基于“持续运营”的设计理念，通过数据资产梳理、数据合规管理、安全能力管理等核心功能，建立“协同管理”的能力，规避产品在实际应用过程中的粗防护、弱联动、单视角等问题。具体功能点包括：

（1）数据资产梳理：盘点数据资产分布、使用和敏感数据流转情况，聚焦业务数据处理活动潜在的安全问题；

（2）数据合规管理：建立合规库，管理合规要求并将其分解为业务数据安全指标，为数据安全运营活动提供输入与参照；

（3）安全能力管理：具备对组件、日志、策略中心的集成管理能力，接入、集成多个安全产品，并针对不同业务的数据安全问题进行策略编排、下发，实现联动防御；

（4）协同关联分析：采集各安全设备和三方厂商安全事件信息进行关联分析，建立资产画像、身份画像等威胁模块，提升风险感知效率；

（5）自动安全运营：建立自动化的运营机制，能够自动根据流程分配运营任务，汇总数据安全风险或事件处理结果。

未来，数据安全运营管理平台**一是要契合组织业务场景，**与组织数据安全建设实现同步规划、同步建设、同步使用，前置组织数据安全运营工作的规划环节，避免简单工具堆砌带来的“拼盘式”运营；**二是要持续沉淀各行**

业、组织的典型业务模型，有效覆盖用户关键业务节点，保障数据安全运营工作效能、效率。此外，数据安全运营管理平台的设计与应用需要持续关注系统性和协同性，一方面持续完善安全工具、安全能力间的可扩展性、兼容性，另一方面强化团队间的协同联动能力，基于不同角色提供多维运营视角，实现从单纯面向威胁的安全运维走向全面、动态的数据安全运营管理。

（九）安全合规服务：咨询与评估成为业内焦点

数据安全合规服务发展向好、需求猛增。目前数据安全合规已成为业内重点话题。2023年《关于促进数据安全产业发展的指导意见》强调壮大数据安全服务，面向数据安全合规需求发展规划咨询服务。可以预见，数据安全合规服务市场发展将持续向好。同时，组织日常经营与发展衍生的大量数据处理活动，亟需借助专业机构的力量，将庞杂的监管要求转化为内部安全策略，数据安全合规服务也因此成为国内数据安全市场的基础性服务，需求量快速增长。

用户对数据安全合规服务寄予厚望。数据安全推进计划《2022年数据安全行业调研报告》显示，89.9%的组织开展数据安全建设的目标已不再是单纯应对监管要求，而是期望完善自身的数据安全合规体系，保障业务发展与数据价值变现。根据图谱数据，25.9%的厂商提供数据安全合规相关服务，主要覆盖数据跨境合规、隐私合规管理、风险监测等重点领域，协助组织强化数据安全保护与合规使用能力。此外，目前组织对数据安全合规服务机构的经验、资质方面的要求逐渐提升：组织不仅关注服务机构是否具备法律、咨询方面的执业资质，还关注服务机构是否在其所在行业具备数据安全合规项目交付经验、优质案例。

数据安全合规服务主要包括咨询与评估两种服务形式。二者在服务过程中的工作重点不同。数据安全合规咨询分为建设性咨询、整改性咨询，两种咨询均侧重于向组织提供可落地的数据安全建设或问题整改方案，重点关注组织数据安全合规遵从能力的提升；数据安全合规评估则主要通过对标特定的法律法规、政策文件，评估组织是否存在合规风险或是否满足特定合规要求。**两种服务形式相辅相成。**在建设数据安全合规体系的目标下，组织通常先开展合规咨询，完善数据安全合规体系，并通过合规评估校验咨询项目的建设效果；在针对特定合规风险开展排查整改的目标下，组织则需要先基于合规评估识别潜在的问题与风险，并通过合规咨询对评估项目发现的问题与风险进行整改。

常见的数据安全合规服务包括重要数据风险评估、数据出境安全评估、数据安全风险评估/咨询，具体服务重点如下：

（1）重要数据风险评估：针对重要数据处理者，聚焦重要数据处理者所掌握的重要数据，梳理重要数据的类型、量级、相关的数据处理活动，并以评估的形式排查重要数据面临的数据安全风险及组织当前的应对措施，识别组织在重要数据识别与管理方面的合规问题；

（2）数据出境安全评估：关注组织的数据出境活动，识别组织业务中涉及数据出境的具体场景，梳理组织出境数据的规模、范围、种类、敏感程度，结合境外接收方责任义务及其数据安全管理与技术措施、能力等信息，分析组织数据出境面临的数据安全风险及组织当前的应对措施，评价组织数据出境活动的合法性、正当性、必要性；

（3）数据安全风险评估/咨询：数据安全风险评估关注组织的数据安全风险，识别组织业务中关键数据资产在各应用场景下的数据安全风险，基

于数据安全风险评估的原则与实施流程，识别数据安全风险的基本要素，并依据风险分析模型对数据安全风险进行识别与评价；数据安全风险咨询则通常衔接组织前期风险评估的结果，侧重于组织数据安全风险接受准则的建立、风险处置策略与措施的制定、落实，实现组织数据安全风险的闭环管理，确保帮助用户建立持续满足监管要求的能力。

未来，数据安全合规服务将贯穿组织数据处理活动，实现组织业务场景的全面覆盖。而且随着合规检测工具的自动化水平提升，合规评估将逐步从“纯人工、周期式”的服务模式走向“半自动、常态化”的服务模式。此外，随着全球数字经济飞速发展，越来越多的组织发展跨境业务，数据安全服务机构也应持续强化对国际、国内法规标准的解读与贯标能力，从而为组织数据出境安全合规提供专业指导。

合规咨询则对服务机构的咨询能力提出了更高的要求：一方面数据安全合规体系建设是一项系统工程，这要求服务机构不仅要懂合规、懂安全，还要懂业务，能够面向各行业、业务场景设计、落实行之有效的专业解决方案；另一方面随着用户对数据安全合规咨询服务的认知持续提升，业内针对数据安全服务机构及其能力的标准及服务实施细则也将不断完善，这也要求服务机构在前期规划、中期实施以及后期运营等方面持续完善自身服务的规范性，提升服务质量，从而在数据安全产业发展浪潮中夺得先机。

（十）分类分级服务：逐渐演变为独立服务品类

数据分类分级是数据安全治理的关键一环。不同类型的数据遭到篡改、破坏、泄露对国家安全、公共利益、公民或组织合法权益造成的危害程度不同。数据分类分级在数据安全治理中起到承上启下的“抓手”作用：数据分类分级通过盘点、梳理不同类型的数据，将数据划分至不同的安全级别，判断不同级别的数据适用的流动范围，从而配置差异化的安全策略，实

现对数据的精细化保护，为数据安全治理筑牢基础。

数据分类分级已成为一项数据安全服务。数据分类分级因其与法规、业务活动的强耦合属性，现已在数据安全服务市场中形成独立的服务品类，并呈现出“咨询为主，工具为辅”的交付趋势。数据分类分级服务的主要内容包括：制定数据分类分级标准、设计数据分类分级策略、形成数据分类分级清单等。图谱显示，12.9%的厂商向用户提供了数据分类分级服务。厂商基于前期在数据治理领域的咨询经验，辅以自动化数据分类分级产品工具，通过“平台+服务”的一体化解决方案，打通业务、系统壁垒，优化组织数据管理生态，提升数据安全协同能力。

图12 图谱：数据分类分级服务

专业咨询是数据分类分级服务的首要增值点。由于组织业务及数据持续高速增长、动态变化，相较于对组织数据的分类与定级，用户更加关注数据分类分级服务能否为组织数据分类分级后的常态化运营工作贡献价值。这意味着服务机构在提供数据分类分级服务时，不应停留于能够向用户交付数据分类分级清单的层面，而是能够充分理解用户的行业属性、业务流程、安全需求，基于业务的数据处理目标开展用户数据资产盘点，设计分类

分级规则与相应安全策略，通过数据分类分级工具自动化识别、标记数据，最终实现数据分类分级结果与组织数据安全策略工具的持续联动。以上内容的实际落地效果与服务机构在实地调研、需求分析以及用户访谈环节的专业程度密不可分，因此专业咨询在数据分类分级服务的价值凸显。

服务机构应持续完善服务流程，辅助用户建立数据分类分级“规划-实施-运营”的闭环管理机制，提供覆盖数据资产清单、安全防护协同、自动化工具的全套解决方案，实现新增或变更的业务数据能够基于业务、安全需求变化进行适配或动态调整。同时，服务机构还应持续提升服务质量，在咨询层面强化规划阶段的需求分析与现状调研，提炼关键的数据交互逻辑，设计贴合用户业务需求与场景的安全管控策略与措施；同时持续提升对各行业领域数据分类分级标准的解析能力，能够基于用户特定业务场景，识别或融合多监管部门、行业的数据分类分级要求，设计符合国家、行业监管要求的数据分类分级规则与流程。

此外，服务机构还需持续提升数据分类分级解决方案的技术能力，应通过引入机器学习、人工智能技术，自动提取数据特征信息，挖掘组织数据之间的规律，构建、优化多种数据分类分级模型，提升数据分类分级工具的性能、效率与精度，提供更高质量的数据分类分级解决方案。

附录

本部分为参与本报告的十家数据安全厂商及其数据安全产品布局与服务理念的简要介绍。

本部分内容由受邀数据安全厂商提供，数据安全推进计划负责整理，以作为本报告相关观点的参考信息。

(一) 综合型厂商

奇安信

奇安信科技集团股份有限公司（以下简称“奇安信”）成立于2014年，专注于网络空间安全市场，为政府、企业用户提供网络安全产品和服务，目前覆盖了98%以上的中央部委、地方政府、中央企业、大型金融机构等重要客户。2022年奇安信成为北京冬奥会、冬残奥会的独家网络安全服务商，并创下了奥运会网络安全“零事故”的世界记录，也是北京市第一批“隐形冠军”企业。2021年，奇安信对外发布了“数据安全能力框架”和“数据安全运行构想图”（数据安全ConOps），为大型政企客户及业内伙伴提供了一套完整的思路、方法和工具，以及配套措施。

奇安信一直以科技创新为驱动力，数据驱动安全、内生安全、新一代网络安全防护体系，引领了我国网络安全行业的发展方向。获世界互联网领先科技成果奖1次，国际信息社会世界峰会(WSIS)奖1次，国家保密科技进步奖二等奖1次，北京市科技进步二等奖1次、三等奖2次，中国通信学会科技进步二等奖1次。

产品布局

奇安信以支撑数据安全体系架构建设为目标，围绕数据安全及新型基础设施安全防护需求，奇安信系统规划、布局了全面的产品和服务体系。其中，特权管理系统、API安全、数据安全态势感知、数据脱敏、数据库审计等6项品类通过业内权威认证。

图13 奇安信数据安全产品布局

服务理念

奇安信的数据安全服务从顶层设计出发，通过咨询规划服务帮客户绘制出数据安全建设的蓝图和体系化建设的路径，通过数据安全治理服务帮助客户建立健全数据安全管理组织制度，落实分类分级、制定相应的数据安全策略和技术保障措施，同时在客户数据安全建设的不同阶段提供针对性的专项安全服务，如前期的安全合规、技术风险识别，数据跨境安全评估、App　隐私合规等，帮助客户做到快一步了解风险为后续做好应对措施建立前提基础；为客户提供数据泄漏事件的安全监控和应急响应，帮助客户第一时间掌握泄漏事件，规避风险，并积极对事件进行溯源，找出泄露点，从根本上解决问题。

图14奇安信数据安全服务框架

（1）数据安全咨询规划服务:通过对组织的业务现状、数据现状、安全能力现状进行分析，以组织 的 IT 战略、业务战略、合规、治理和风险容忍度作为输入制定数据安全战略，以数据安全能力 框架为指引从管理、技术、运营三个维度进行体系化设计，给出用户数据安全建设能力的全景和实施路径，指导数据安全建设的工程化落地。

（2）数据安全治理咨询服务:帮助用户厘清监管/合规要求，建立健全数据安全管理组织、制度流程 规范，厘清数据资产、落实数据分类分级，梳理清楚数据的流转和访问关系，制定相应的数据 安全策略和技术防护保障措施，帮用户梳理清楚数据安全保护的对象和体系化建设的路径。

图15奇安信数据安全服务流程

(3) API接口数据泄漏技术评估:采用渗透手段,模拟黑客攻击,深度发现当前对外API接口存在 数据泄漏的安全风险,包括敏感信息泄漏、错误配置、注入漏洞、弱身份鉴别、弱会话控制、越权等风险。

(4) 数据安全蓝队评估:模拟APT攻击手段,以获取客户核心数据(客户定义)为目标,深入评估 客户数据安全防护的短板。评估过程模拟入侵杀伤链,评估方法包括网络攻击、社会工程攻击、近源攻击等。具体的场景可以模拟勒索病毒、拖库等。

(5) 数据库安全评估:针对涉及存储企业敏感数据的大数据平台或者数据库系统,对账号权限管理,系统存在的弱口令、系统漏洞、安全选项配置等技术情况进行综合评估发现其存在的安全 隐患。

(6) 数据渗出防护能力评估:以ATT&CK为理论模型,聚焦数据渗出阶段的攻击行为,验证现有防 御体系对网络入侵引起的数据外泄行为的可见性(不可见、只有告警、可防护)。

(7) 数据安全合规评估:依据网络安全法、数据安全法等法律法规对客户数据进行全面合规性评估,评估领域包括机构人员、制度保障、权限管理、应急处置、安全审计、数据加密、核心数据处理保护、个人信息保护等 21 评估域及 269 项列表。

(8) 数据安全风险评估:参照GB20984标准,依据数据资产、数据应用场景、数据威胁、数据脆弱性、安全措施等评估要素对客户数据进行全面的安全风险评估。

(9) 数据安全成熟度评估(DSMM):通过组织建设、制度流程、技术工具、人员能力4个维度, 依据《信息安全技术 数据安全能力成熟度模型》对客户数据进行安全成熟度评估。

（10）数据泄漏信息监控:依托平台，以外部视角，持续监控非公开网络数据泄漏信息源，实时推送 客户资料/用户信息泄漏信息，并定期提供数据泄漏阶段性报告。

（11）在2022北京冬奥中，奇安信制定了一套盘清家底、分级分类、精准防护的三大步骤数据安全完整方案，使得整个冬奥期间未发生一起数据泄露事故，兑现了“零事故”承诺。

图16 奇安信数据分类分级服务流程

亿赛通

北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）成立于2003年，是国家双高新企业、工信部认证的“专精特新”小巨人企业。深耕行业二十年，亿赛通以“助力国家大数据战略、保障数据资产安全”为己任，提出“制度主建、技术主战、分放管服”的安全理念，提倡“数据分权分责分风险、放权管责相结合”，在保障安全的同时实现数据价值的最大化，为政府、金融、运营商等十余个行业提供专业的数据安全产品和服务。

产品布局

亿赛通以安全服务、产品方案、工程交付三个体系为主导，以“分（分层治理、制度先行、技术支撑）、放（简化流程，让数据按需放心流转，产生合理价值）、管（技术监管、放管结合，促进数据安全流转）、服（高效服务，营造及时管理环境；立体运营，保障数据安全）”为数据安全建设理念，对商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行各业核心数据资产安全。

匠心打磨二十载，亿赛通的数据安全产品深度融合人工智能、大数据、区块链、5G等新兴技术，支撑云、网、端全场景，覆盖数据安全审计检测、加密防护、安全管理、安全平台、安全服务全品类，形成以“数据安全流转为中心”的智能化、一体化、专业化的解决方案。

在数据安全防护上，产品能够将结构化、非结构化和半结构化数据作为防护对象，对电子文档、数据库进行全方位、多维度管理。在终端侧，基于数据内容进行全量、增量、一次性、周期性扫描，对数据内容进行识别与检测，

按照数据分类分级标准制度，对数据进行分类分级管理，实现加密、外发审计、审批和阻断等管理措施；在网络侧，内置全球IP地址库，将数据访问发起端和响应端进行IP地址比对，识别数据的违规流转、跨境传输、非法处境行为和数据信息，并进行审计记录、风险告警及流转阻断限制；针对数据分散存储的状态，在终端、服务器端、云虚拟环境、网络端、邮件端支持全覆盖多点部署，为企业提供数据安全保障。

在数据安全流转上，产品通过存储加密、数据变形、访问控制、行为监测等技术手段，针对开发测试环境、数据交换、数据分析、数据共享等情况下的敏感数据进行批量化处理，防止外部黑客攻击、内部数据窃取、脱库等风险下的数据泄露。遵循数据安全合规建设，保障数据存储、流转过程中的安全存储与按需放心流转。

图17 亿赛通数据安全产品布局

服务理念

亿赛通基于数据安全合规要求与数据安全风险治理专业实践，以服务的形式向组织用户提供咨询规划、评估认证和安全运营支撑，通过聚焦核心业务和关键需求，摸清全量数据和权属关系，分析安全风险和治理空间，提升运维保障和人员能力，帮助客户改善“信息化建设”与“安全建设”双规并行，“安全管理”与“安全技术”衔接不畅的问题，实现数据安全状态的可持续保障。

亿赛通的数据安全服务已覆盖政府、央企、金融、能源、智能制造等多个行业领域，在数据安全风险评估、数据资产盘点、数据分类分级、数据防护策略搭建、数据安全检查、数据安全培训乃至全面的数据安全治理工作中积累了丰富的实践经验。面对国家、地区、行业发布的百余项数据安全合规文件要求，亿赛通帮助客户实现准确对标和深入理解，并将理论要求和实践经验落实到具体工作中，为用户的信息建设和数据管理工作保驾护航。

以中国外运股份有限公司（以下简称“中国外运”）的数据安全体系建设咨询项目为例，亿赛通按照中国外运的整体网信安全管理和技术防护体系规划，以业务高效开展和数据安全流通为目标，以“风险防范”与“安全合规”为抓手，打造了中国外运数据安全保护体系。亿赛通通过“一个战略规划”、“两个安全支点”、“三个行动方向”、“四个能力维度”的治理思路，以及为期三年有序推进的实施计划，实现中国外运网络安全、数据安全、业务安全的一体化组织保障，以及数据安全核心能力的稳步提升。

图18 亿赛通数据安全服务案例

保旺达PROWADA 保旺达

江苏保旺达软件技术有限公司（以下简称“保旺达”）江苏保旺达软件技术有限公司是一家提供专业数据安全产品及安全服务的国家级高新技术和专精特新企业。公司以“创造更安全的数字未来"为使命，基于自主创新技术做精做深全系数据安全产品，为政府、运营商、军工、金融、能源等行业用户和各类型企业用户提供安全、合规、全生命周期、全业务场景的数据安全整体解决方案和服务，为国家数字强国、制造强国战略以及企业数字化转型提供坚实的网络安全基础与数字安全保障。

产品布局

图19 保旺达数据安全产品布局

合规和安全双轮驱动，夯实数字安全底座。保旺达以“合规和安全双驱动”为核心理念构建数据安全整体防护生态，围绕数据安全防护、数据安全流通和数据监管合规三大目标，从运营体系、合规体系、管理体系、技术体系和组织体系为企业的数字化转型保驾护航。

十大专项能力支撑，构建全链路数据安全运营平台。保旺达基于IAM和PKI两项通用能力，以数据资产梳理系统、接口安全管控系统、文档安全流转中心等十大专项能力系统为支撑，搭建了数据安全运营管理平台、数据安全共享和流通平台、数据安全监管合规平台以达成生态目标。

全场景数据分类分级，多维度绘制数据资产“动”、“静”地图。数据资产梳理系统协助企业理清数据资产现状、明确数据安全治理目标，为企业制定数据安全方案提供支撑。系统采用流量监测和主动检测等多种技术手段，自动发现数据源和数据资产，尤其是存储的暗数据。系统采用自动识别和人工稽核相结合的方式对所有数据进行分类分级，生成完整的数据资产清单。同时从数据的分类、分级、分布、存储、流转、安全措施等多维度绘制数据资产“动”、“静”地图。另一方面，针对上级监管单位的考核要求，数据资产梳理系统提供了辅助生成分类分级清单、重要/核心数据清单、数据安全态势报告的能力，方便安全管理员及时、高效的应对考核。

图20-1保旺达数据安全产品架构（数据资产梳理系统）

安全监管流转数据，释放数据要素价值。接口和文档是数字化企业中数据流转的最主要途径，针对这两种途径，保旺达提供了接口安全管控系统和文档安全流转中心，以保障数据在流转过程中的安全，降低数据泄漏风险。

（1）接口安全管控系统。帮助企业梳理接口资产并检测其脆弱性，对接口访问进行持续监测、审计和多维度管控。系统自动发现、分类网络内暴露的接口并按应用系统归集，生成接口资产台账，同时结合IP情报和接口行为模型对接口进行分类，自动识别敏感数据访问接口、跨部门数据共享接口、僵尸（失活）接口等，实现对接口资产的集中化管理，提升管理效率，避免错漏。同时通过独立部署的接口网关，为接口提供“外挂”式的安全防护能力，提升接口和传输数据的安全性。为解决因接口升级、降级等导致的接口变更及风险变化，接口安全管控系统采用版本化管理模式，记录接口的每个版本特征，结合持续监测能力，主动发现版本不一致的接口。在检测到已备案接口发生变化时，系统会立即检测新接口的脆弱性，生成脆弱性分析报告，并提供相关的安全防护建议。

图20-2保旺达数据安全产品架构（接口安全管控系统）

(2) 文档安全流转中心。为企业提供了文档可控流转的途径、加密的文档存储和在线协同编辑能力，避免了涉敏文件落到不可控终端而导致的数据泄漏。当应用/用户在系统中创建新文档后，系统会自动对文档内容进行扫描，分析文档涉敏情况。同时为文档属主提供了对文档生命周期的管控能力，支持对文档流转后的权限进行控制，包括重命名、移动、复制、编辑、查看、转发等。且可根据特定动作触发文档的自动销毁，如，查看指定次数、转发、下载等。对于某些必须要下载到终端的文档，会根据策略对文档进行脱敏、加密、水印、金库审批等防护。文档安全流转中心采用区块链和文件指纹技术记录文档的流转和变化过程，并通过文档关系图，方便安全管理员对文档进行跟踪和溯源，防止恶意抵赖。

图20-3保旺达数据安全产品架构（文档安全流转中心）

服务理念

保旺达秉持“安全合规、防范风险、闭环管理、数字化运营”的服务理念，以“符合监管要求和考核要求、发现和防范实际的安全风险和问题、围绕数据生命周期和业务流程实现安全闭环管理、服务效果能够数字化呈现并持续改进”的服务目标，基于以“安全合规，防范风险”为指引，坚持“平台+产品+服务”的整体服务思路，向企业提供优质的数据安全服务。

保旺达注重“实战化，平战结合”，将国家数据安全合规要求和上级单位考核要求融入各项评估项和服务项，围绕数据采集、存储、使用、加工、传输等全生命周期及数据流转相关业务流程提供完整的数据安全服务。将国家数据安全合规要求和上级单位考核要求融入各项评估项和服务项。

以电信某省分公司的数据安全评估服务为例，保旺达通过数据安全评估平台工具能力和专业的数据安全评估服务团队，依据该平台提供的数据安全评估的流程化、体系化能力，为数据安全评估工作提供了坚实的技术保障。

保旺达的数据安全服务团队通过“确定范围-需求解析-风险评估-风险研判-整改建议、复评-提升”的全套服务流程，一方面帮助客户定期完成重要数据处理活动开展数据安全风险评估，按年度提交数据安全风险评估报告，满足部委、集团的合规与考核要求，另一方面为电信省公司数据安全管理工作进行梳理、分析、验证、总结及持续改进，及时发现安全风险，避免数据泄露事件发生，实现闭环管理。为数据安全建设及改进提供依据，提升数据安全管理能力。

图21 保旺达数据安全服务案例

(二) 专业型厂商

安恒信息

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于2007年，于2019年登陆科创板。安恒信息专注于数字安全领域，秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，致力于成为全球领先的数字安全企业。

安恒信息凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系。作为国家级的核心安保单位，安恒信息参与了国家重大活动的网络安保工作：2020年11月23日，安恒信息正式成为2022年杭州第19届亚运会网络安全类官方合作伙伴，开展国际大型综合性赛事网络信息安全类最高层级合作。

产品布局

安恒信息现已形成覆盖网络信息安全生命全周期的产品体系，各产品线及业务线在行业中均形成了强大的竞争力。在数据安全保障能力建设方面，安恒信息已建立“安恒数盾数据安全整体解决方案”，通过加强核心技术攻关，优化升级数据识别、分类分级、数据脱敏、数据权限管理等共性基础技术，夯实数据安全基础。同时，加强隐私计算、数据流转分析和全链路数据安全管控等关键技术，依托数据安全咨询规划和“CAPE”技术能力框架，建立覆盖数据全生命周期的安全防线，并最终形成自闭环的“数据安全运营”能力，实现“整体智治”的安全目标，激活数据潜能，释放数据价值。

图22 安恒信息数据安全产品布局

服务理念

数据安全服务是安恒数据安全战略的主要发力点之一。安恒信息持续在服务理念、实践突破、案例沉淀、专题创新、标准布局、战略合作、品牌打造等方面持续优化自身能力，力争向客户呈现坚韧开拓精神，为未来稳步迈进新台阶夯实基础。

（1）服务理念进化：立足三体系、三协同、三服务。安恒信息围绕数据安全防护、管控、监管三大协同机制，作用于数据安全管理、运营、技术三大体系架构，提供输出面向数据处理支撑、使用、共享交换利用的三大安全服务领域，持续为客户提供管理抓手、技术赋能、运营联动，保障全链路全场景全周期的数据安全。

（2）服务实践突破：八大核心、八项运营。安恒信息基于咨询理念和落地实践发布八大类核心咨询服务：数据安全顶层规划、数据分类分级、数据安全合规评估、数据安全能力成熟度（以下简称DSMM）评估、数据安全风险

评估、数据安全治理咨询、防泄密体系建设、数据安全运营体系设计咨询服务。

图23 安恒信息数据安全服务框架

安恒信息联动“安恒数盾”全系产品推出八项运营细项服务：数据安全分类分级运营、风险管理、访问权限管理、策略管理、威胁监测、应急响应、隐私合规、及审计运营服务，不断夯实核心服务基座，逐步形成安恒信息数据安全服务全景图。

图24 安恒信息数据安全细项服务简介

（3）服务案例沉淀：重要行业全覆盖。2022年，安恒信息继续保持政府大数据局行业案例优势，新增积累部委、省厅级专业政府机构案例，攻坚突破大型央国企、交通行业，重点打造运营商及金融行业数据安全服务标杆，开拓医疗、教育行业市场，通过咨询服务结合产品技术实践，融合数据治理、隐私保护、网络安全等多重体系，帮助行业客户持续提升数据安全体系规划建设和运营水平。

（4）专题服务创新：基于业务的数据安全风险评估。安恒信息通过整合重点行业内客户真实需求、已有评估框架与安恒信息九维彩虹团队中红队、紫队能力，梳理全过程闭环评估逻辑，充分发挥API监测审计、敏感数据发现、安全开发需求平台等工具的技术能力，创新开发数据安全风险评估服务，同步实战不断积累，形成数据安全风险知识库。

（5）专业标准布局：积极参与标准制定与修订工作。安恒信息作为主要参编单位积极参与《大数据 数据安全风险治理成熟度模型标准》《电信网和互联网数据安全评估规范》《信息安全技术 网络数据分类分级要求》等标准的编写、修订工作，持续感知数据安全领域发展新趋势，增强行业影响力，拓宽数据安全发展视角，建立业内良性互动。

美创科技

杭州美创科技股份有限公司(以下简称“美创科技”) 于2005年由国内多名数据库资深专家携手成立，公司总部位于杭州，在全国32个省市设立分支机构，是国内领先的数据安全和数字化转型产品服务提供商。美创科技目前拥有数据安全、数字化转型、运行安全三大业务及数据安全运维服务，研发形成数据分类分级、数据安全防护、数据安全审计、数据安全运营、数据资产管理、数据库运行安全、灾备集中管控等30余款产品，已服务政府、金融、能源、运营商、医疗、教育、企业等行业领域的万余用户。

产品布局

美创科技以韧性理念、零信任2.0架构、入侵生命周期、风险评估为基础，主张以灵活的安全策略，基于资产、身份、风险，构建由内而外的“韧性”数据安全防护体系，通过对数据在存储域、流动域、访问域等各个领域落实有效安全管控措施，实现复杂系统可见，快速的感知、干预和恢复，让数据在遭受威胁时能快速响应、攻击发生后快速恢复，同时通过适应性进化持续保障身份和资产全生命周期的安全。

图25 美创科技数据安全产品能力全景图

美创“韧性”数据安全产品体系下的典型产品包括：

（1）数据库透明加密系统。在保障业务系统透明访问的前提下，实现数据加密存储，根据用户权限返回明文或密文数据。

（2）诺亚防勒索系统。主动识别和发现未知风险，抵御勒索病毒、挖矿病毒等常见病毒。

（3）数据库防水坝。保证敏感数据资产可管、用户访问行为可控、返回结果可遮盖，实现数据库运维安全管控。

（4）数据库防火墙。抵御并消除由于应用程序业务逻辑漏洞或缺陷所导致的数据(库)安全问题，保护数据库免受外部入侵攻击。

（5）动态数据脱敏。基于身份权限对敏感数据实时脱敏，实现敏感数据去隐私化展示。

（6）数据库安全审计。通过深度解析网络流量中的数据库协议，还原数据库操作行为，为安全事件提供溯源依据。

（7）静态数据脱敏。自动发现敏感数据，对敏感数据进行漂白、变形、遮盖等去隐私化处理，并保持业务特征和关联性。

（8）数据水印溯源系统。对数据文件中的内容进行全自动读取、识别、变换、增加水印，实现数据泄露后溯源追责和版权宣示。

（9）API安全监测与访问控制系统。基于分类分级结果，全面梳理应用及API接口资产，实现敏感数据流动风险监测与细粒度访问控制。

（10）暗数据发现和分类分级系统。自动进行数据发现、数据含义识别、数据分类分级，并具备目录化管理和可视化分析能力，实现高效持续化盘点数据资产。

（11）数据安全管理运营平台。从真实业务场景出发，围绕资产、身份、

策略和业务，进行资产规范管理、安全多端联动、运营增值，实现资产全域可管、风险全域可视、策略全域联动。

服务理念

美创科技数据安全服务包括数据安全治理咨询服务、数据安全运维服务、数据安全运营服务。以专家级支撑服务体系，以自动化工具赋能，从“知、建、管”三方面，构建咨询到规划，再到持续安全运营的服务闭环。

（1）数据安全咨询服务。着眼解决用户存在的数据安全“需求不明确、责任不清晰、管理不规范、建设不匹配”等一系列问题，参考业内知名数据安全治理理论模型（DSG、DSMM等），结合CARTA、IPDRR、PDCA方法论，形成切实可落地的数据安全治理实践路径。目前，数据安全治理服务既包含整体治理咨询服务，同时提供数据分类分级咨询、数据出境安全评估、数据安全风险评估、个人信息风险评估等专项服务。

图26 美创科技数据安全咨询服务体系

（2）数据安全运维服务。确保数据可用性和完整性、兼顾机密性，通过运维和安全两类服务，保障业务连续性。服务包括：数据基础环境故障处理、运行安全保障、数据安全漏洞扫描、安全加固、渗透测试、安全基线检查、安全培训以及安全通告等服务项目。

图27 美创科技数据安全运维服务体系

（3）数据安全运营服务。依托数据安全管理平台，构筑数据安全运营服务能力，逐步落实组织长期数据安全目标，实现风险监测常态化、数据资产清晰化、应急处置流程化等目标。数据安全运营服务包括重要保障服务、风险监测服务、应急处置服务和常态化安全检查等服务项目构成。

图28 美创科技数据安全运营服务体系

炼石网络

北京炼石网络技术有限公司（以下简称“炼石网络”）是一家数据安全技术创新厂商，先后获得安天、国科嘉和、腾讯、重庆科技成果转化基金等投资，面向个人信息和商业数据保护等场景，开创自研“免改造数据安全”产品，并为客户提供专业的数据安全服务。炼石免改造数据安全技术特色是免开发改造应用的数据保护、高性能国产密码和去标识化技术，为政府、金融、运营商、交通、教育、医疗、文旅、工业等用户提供个人信息保护、商业数据保护、数据安全合规改造、国密合规改造。

产品布局

炼石网络秉承以“数据为中心”的新安全理念，坚持原创自研和持续迭代，致力打造免改造应用的数据安全产品体系，目前已形成包含“一平台（数据安全主平台）、多模块（识别、防护、检测/响应、恢复、审计/追溯以及安全合规等安全能力模块）”的数据安全产品矩阵，可通过高覆盖率的数据控制点，横向覆盖广泛应用、纵向叠加多阶安全能力，有效保护结构化与非结构化数据，实现集中式管控、分布式保护，可应用于数据收集、存储、使用、加工、传输、提供等环节。其中，炼石网络的数据安全主平台开创性地基于面向切面安全技术，实现免改造应用的细粒度数据安全防护，可覆盖应用系统、数据库、文件系统、磁盘、终端等数据流转的多层级，具有免改造应用交付快、应用架构兼容广、密码安全一体化防护强、适应业务数据流向管控准等优势。

炼石网络的产品方案可在不影响业务的前提下敏捷实施上线，将安全与业务在技术上解耦、但又在能力上融合交织，实现主体到应用内用户、客体到字段/文档级的有效保护，打造实战化数据安全防护体系。目前，炼石网络已形成了成熟标准化产品与交付体系，能够满足政府、金融、运营商、教育医疗文旅、工业等行业客户，在个人信息保护、商业秘密保护、数据安全合规改造、国密合规改造等业务场景需求。

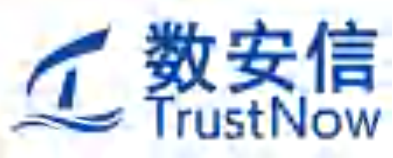
图29 炼石网络数据安全产品矩阵简介

在免改造应用的数据安全产品体系基础上，炼石网络进一步强化配套服务体系，打造4项通用服务和2项专项咨询服务，致力于满足企业和组织发展战略、合规要求和风险治理等诉求，让数据安全防护成效实现“1+1>2”。

（1）数据安全通用服务包括数据安全规划、数据安全建设、数据安全运维和数据安全培训。其中，数据安全规划主要是协助用户明确数据安全目标，通过对平台、价值、体系、指标、防护能力等路径，结合不同行业的合规要求和风险要素，为各行业用户提供适配、全面、针对性的整体规划；数据安全建设主要是帮助用户打造涉及监管层、能力层、数据层的实战化技术体系；数据安全运维主要以风险管理为核心，结合安全防护技术手段，保障用户业务可持续性；数据安全培训主要是从法律法规、安全事件、形势分析、安全防护和行业实践等方面开展讲解，帮助用户掌握行业数据安全管理理论依据和具体实践要求，持续做好数据安全体系建设工作。

（2）数据安全专项咨询包括DSM数据安全管理认证和PIP个人信息保护认证。当前，我国数据合规领域认证制度重点已经从产品安全、技术规范逐步扩展到组织体系、管理流程等综合治理层面，并形成了对个人信息与重要数据有效保护的完整合规基线。炼石网络的数据安全专项咨询，主要面向国家市场监督管理总局和国家网信办颁布建立的“个人信息保护认证”和“数据安全管理认证”，从技术角度和管理角度深入分析客户企业数据存在问题，协助用户落实合规、提升实战防护水平。

图30 炼石网络数据安全服务框架



数安信

数安信（北京）科技有限公司（以下简称“数安信”）成立于2021年，专注提供“法律+科技数据安全合规”的一体化解决方案，基于专家团队对数据安全法律法规的深刻理解，结合可信计算、大数据、区块链、隐私计算以及人工智能等科技手段，为客户提供“数据隐私、安全、合规及第三方风险评估与防范”等标准化产品、解决方案及拓展服务。

数安信现已加入包括全国信息安全标准化技术委员会、中国通信标准化协会大数据技术标准推进委员会（TC601）、浙江省网络空间安全协会、杭州数据安全联盟等组织，深度参与数据安全国家标准与行业标准研制，并已申报二十余项技术发明专利及软件著作权等知识产权。核心技术团队成员来自国内知名IT企业，具有二十余年的IT资深从业经历及权威专业资质。

产品布局

数安信围绕数据合规管理能力建设，提供专业的数据合规产品及解决方案。

（1）数据合规信息采集。主要实现对数据安全合规信息的采集，合规数据采集点涵盖数据处理各个环节，包括数据收集、传输、存储、使用、加工、提供和公开等，数据合规采集方式包括数据扫描、API接口报送、网络流量采集和合规问卷调研等多种方式。

（2）数据合规信息分析。主要实现对采集来的数据合规信息进行分析和处理，主要功能包括数据安全法律法规知识库、数据安全合规规则分析与管理、数据安全技术处理的合规分析及数据安全管理的合规分析等。

(3)数据合规监管处置。主要实现对数据合规结果的处理及给上级监管机构的合规数据报送等，主要功能包括合规态势监控、合规分析报表及合规监管数据报送等。

(4)数据合规安全审计。主要实现数据合规监管过程的审计，确保合规监管过程的有效性与合法性，主要功能包括合规信息采集审计、合规信息分析处理审计与合规审计报表分析等。

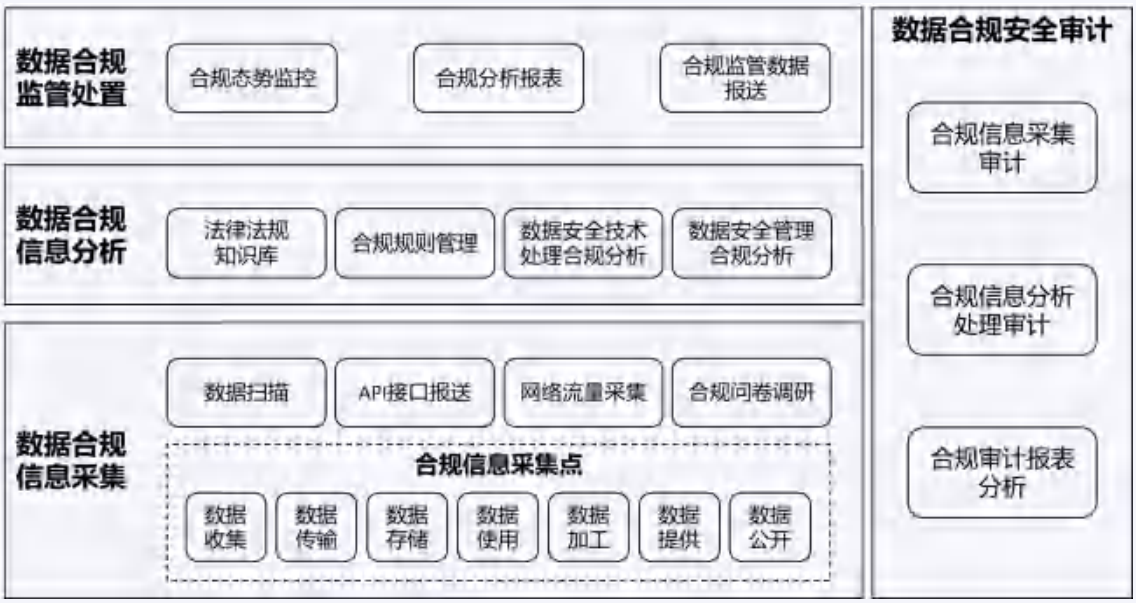


图32 数安信数据合规管理能力体系

服务案例

数安信聚焦数据合规及安全技术领域，提供专业的数据合规和数据安全产品及解决方案，深度参与多项数据安全领域重点课题研究及国家标准、行业标准及地方标准研制，支撑多个国家部委、省级与地市级数据安全项目工作。

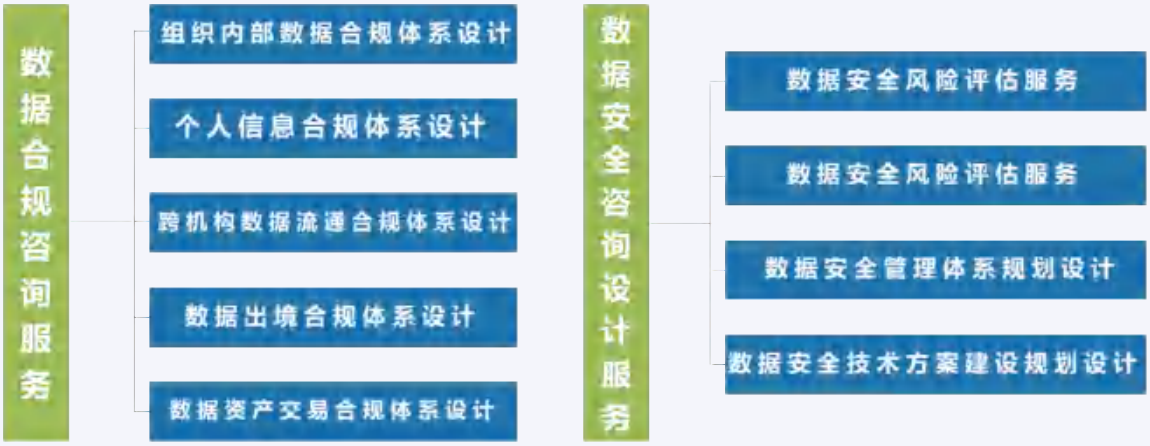


图33 数安信数据安全合规服务框架

数安信承担了我国医学研究领域某数据出境安全评估项目的技术支撑。该项目为北京某医院牵头的国际多中心临床研究课题项目，项目中涉及到我国境内参与项目研究的志愿者个人信息的出境合规和安全保障。数安信作为项目中该医院的支撑单位，承担了跨境研究平台搭建、数据出境合规自评估、项目运营等多项职责。

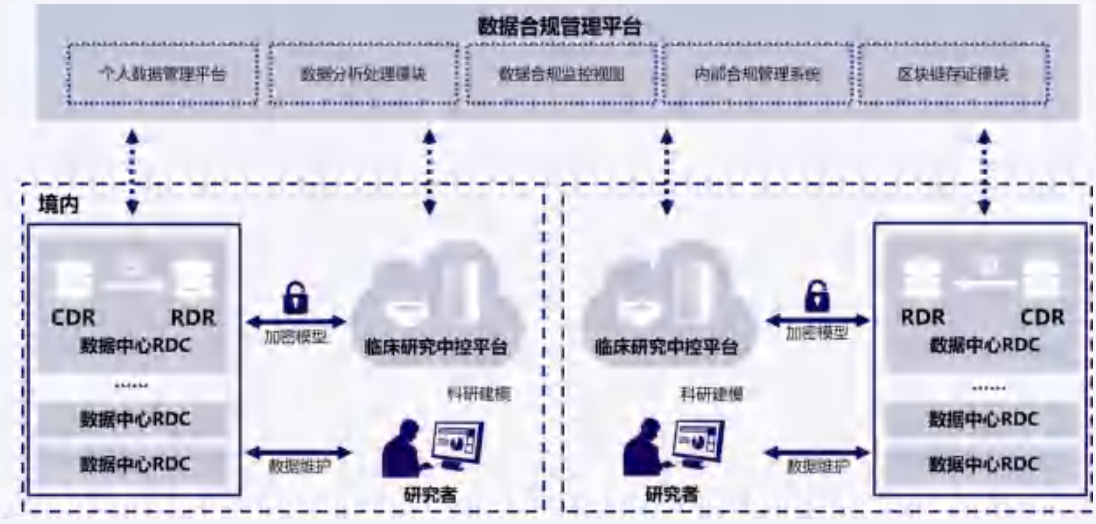


图34 数安信数据安全服务案例

(三) 新兴型厂商

融安数科

神州融安数字科技(北京)有限公司(以下简称“融安数科”)以密码技术为基础,专注于提供专业的隐私计算产品与解决方案。2019年开始,融安数科基于自身在密码学基础领域的深厚积累,深刻洞察数据安全需求与痛点,组织团队进行自研,取得了隐私计算相关多项软件著作权和27项发明专利,并于2020年推出融安隐私计算平台(融安隐私网关)产品,独创了隐私度量技术和合规监管技术,在保证数据流通过程中不泄露原始数据的前提下,对数据进行分析和计算,保障敏感数据在存储、计算、应用、销毁等全流程各个环节的“可用不可见”。

产品布局

针对数据隐私保护需求,融安数科创新推出融安隐私计算平台,综合多方安全计算引擎、联邦学习引擎、联邦统计引擎、联邦分析引擎,结合隐私求交、隐匿查询、联合统计、联合建模、安全分析等技术方案和国产密码安全芯片、定制硬件等技术,在保证数据流通过程中不泄露原始数据的前提下,对数据进行多维分析和计算,保障敏感数据在存储、计算、应用、销毁等全流程各个环节的“可用不可见”。

(1)丰富的隐私算子。支持同态密码、秘密分享、混淆电路、隐私交集、不经意传输、隐私比较等,并在此基础上融合、优化形成丰富的隐私算子

(2)灵活的计算框架。支持数据核验、模型计算等标准业务,也可在隐私度量的基础上支持特定隐私计算业务流程,并支持双机热备和集群管理

(3) 各种计算场景支持。支持各种规则和模型计算，并可根据计算函数类型、实时或批量计算要求、局域网或广域网环境要求、业务并发量及响应时间要求等设计支持不同的计算场景

(4) 搭积木方式快速响应。根据业务场景要求，可采用搭积木的方式组合各种隐私算子，高效、快速、灵活地适应千变万化的业务需求

图35 融安数科隐私计算引擎产品架构

服务案例

2021年中国人民银行发布《关于做好小微企业银行账户优化服务和风险防控工作的指导意见》，要求对小微企业银行账号全生命周期管理，加强涉诈涉赌交易识别管控，加强对存量账户的排查清理和对涉诈涉赌账户的责任倒查。金融集团开展金融业务时，一方面需运用技术手段加强涉诈涉赌交易识别能力，引入外部数据源，拓展数据维度属性来提高金融反欺诈风控模型的精度，另一方面需要遵循国家隐私保护相关法律法规，保证合法合规使用数据。

融安隐私计算平台向该金融集团提供了合法合规使用内外部数据，用于提高反欺诈风控模型精度，加强风险识别能力的解决方案。融安数科提供的解决方案运用多方安全隐私计算技术实现金融集团、运营商、电力公司三方联合计算，输出企业信用评分，用于金融反欺诈场景；同时方案中引入第三方监管机构，运用隐私度量技术、参数一致性监管技术、匿踪计量计费技术等一系列密文监管技术对交易全生命周期合规监管。

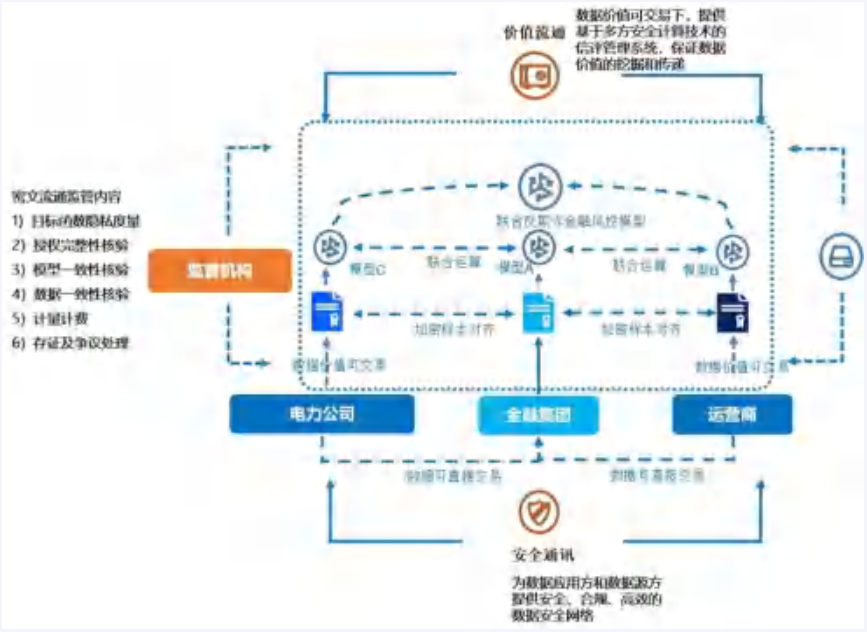


图36 融安数科隐私计算解决方案架构图

该方案使用多方安全计算技术解决了金融集团运用内部数据和外部数据源的数据保护问题，各方数据联合运算，输出企业信用评分，实现风险控制，为金融集团将本增效；如何监管交易合法合规进行，方案中引入第三方监管机构，对于事前、事中、事后监管进行了有益探索和实现。

洞见科技

深圳市洞见智慧科技有限公司（以下简称“洞见科技”）是由信用产业集团“中诚信”孵化、网信事业国家队“中电科”投资的领先的隐私计算技术服务商，致力于赋能数据价值的安全释放和数据智能的合规应用。公司的创始团队是中国大数据征信和智能风控行业的推动者和领军人物，核心成员来自中诚信、大型银行、保险公司、大数据与人工智能企业，具备丰富的行业知识和服务经验。

洞见科技在2020年初推出国内首个面向场景的、隐私计算平台InsightOne，围绕数据资源融合和业务场景应用构建安全可信的数据智能联邦，已经在政务、金融等领域取得了大量商业案例。凭借过硬的隐私计算技术实力和专业的应用落地服务能力，洞见科技已获得IDC中国FinTech 50、KPMG中国领先金融科技50企业、CB Insights数据链路安全领航者、iResearch隐私计算卓越者及金融市场综合领导者等多项荣誉。

产品布局

洞见数智联邦平台（InsightOne）是由洞见科技于2020年初推出的国内首个面向场景的隐私计算平台InsightOne，平台以多方安全计算和可信联邦学习为主计算引擎，以可信执行环境、差分隐私、零知识证明等为辅计

算引擎，通过匿踪查询、联邦建模、隐私求交、联合计算等多种业务场景应用，实现全流程数据隐私保护，以“数据可用不可见、计算可控可链接”的方式帮助政务、金融、通信、能源等行业客户安全释放数据价值。

InsightOne平台拥有面向场景的融合计算引擎、可监管的分布式信任架构、全计算链路隐私安全保护、深入场景的专业算法、无可信第三方联邦学习、匿踪联邦学习、区块链增信网关、多方安全图计算&图联邦学习、跨平台互联互通容器等核心技术优势，具备“安全、融合、兼容、灵活、专业、易用”等产品优势.此外，InsightOne平台是国内唯一全面通过中国信通院多方安全计算和联邦学习功能、性能、安全、辅助工具、金融场景，以及国家金融科技测评中心多方安全计算和联邦学习金融应用等隐私计算全系列评测的产品，并适配主流国产信创芯片服务器及操作系统。

服务布局

洞见科技基于团队多年的政务、金融服务实战经验和行业知识积累，通过隐私计算“基础设施平台建设+业务场景运营服务”的方式已在数据开放、数据交易、银企融资、智能风控、电信反诈、联合营销、存客激活、精准投放、保险精算、资产扫描、债指编制等应用场景实现大量商业化落地。

图37 洞见科技InsightOne平台相关场景解决方案

(1) 在智能风控场景中，在金融机构与外部机构之间构建安全可控的数据协作通道，在原始数据不出域的前提下，使用金融机构内部业务数据和外部合作数据联合构建风控模型，并基于模型进行实时预测，应用于反欺诈、反洗钱、风险评估、风险预警等。

(2) 在精准投放场景中，基于洞见隐私计算平台，在媒体方与业务方之间构建安全可控的数据协作通道，结合营销目标，构建专属投放模型，协助其完成高响应客户的筛选和选择，使得投放更精准，大幅提升投放转化率，降低获客成本。

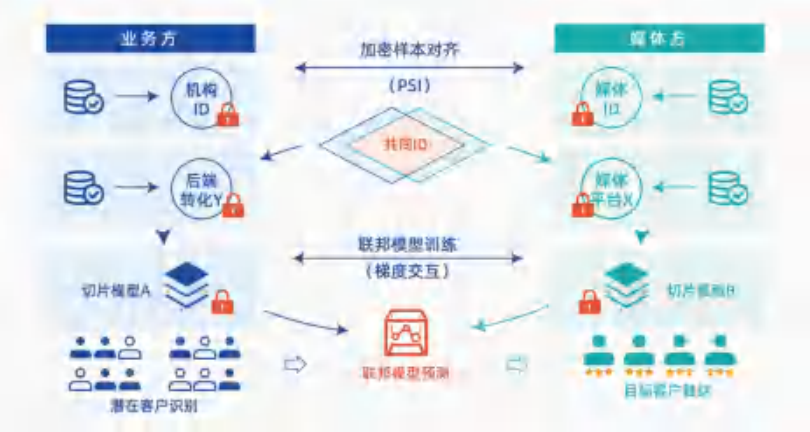


图38 洞见科技精准投放场景解决方案

(3) 在数据开放场景中，解决政务数据既要开放共享又要保护隐私的两难问题，提升政务公共数据存储、计算、应用、通用支撑和服务管理能力以及安全防护能力，促进内外部数据安全融合计算与应用，服务于普惠金融、乡村振兴、供应链金融等场景应用。

(4) 在数据交易场景中，基于洞见隐私计算平台构建数据开放、共享、交换平台，能够以“使用即交易”的方式重构“转移式交易”的数据要素流通市场，结合区块链技术对数据进行确权和资产化的探索，促进政务数据跨层级、跨区域、跨部门、跨行业的流通，以及政务数据面向企业的开放赋能。

图39 洞见科技数据要素安全交易场景解决方案

基于InsightOne平台，洞见科技目前已与国家信息中心、国家工业信息安全发展研究中心、中国中小企业发展促进中心等达成合作，并为山东、湖北、聊城、武汉、安康、洛阳、长春等多个地方政府，中国移动、中国联通、中国电信等通信运营商，国家电网等能源企业，中国银联及多家国有银行、股份制银行、城商行、农商行、保险机构等上百家头部客户落地了众多隐私计算基础设施与场景运营行业标杆案例，始终以专业的技术服务助力隐私信息安全保护、多方数据安全融合及业务应用效果改善。

金智塔科技

杭州金智塔科技有限公司（以下简称“金智塔科技”）是由浙江大学人工智能研究所和浙江大学金融科技研究院联合发起的数据合规流通与应用领军企业，以“让数智世界更可信”为使命，自主研发了隐私计算平台、数据要素流通平台、安全计算沙箱、机器学习平台等产品，为浙江省统计局、浙江省经信厅、浙商银行、宁波银行、郑州商品交易所、美的集团等数十家行业标杆用户提供安全高效的数据流通和数据智能解决方案。

产品布局

金智塔科技自主研发的隐私计算平台融合了多方安全计算、联邦学习、区块链等技术，提供联合建模、联合统计、匿踪查询、在线推理等服务，实现数据“可用不可见”、“用途可控可计量”，赋能数据要素安全高效流通，并促进数据要素的融合创新应用。产品优势包括：

（1）高安全：采用区块链、数字水印等多种技术对数据使用的全链路进行安全防护和存证，为安全提供了深度保障。

（2）高性能：采用分层架构设计，可针对不同的业务场景及环境进行个性化配置与优化，支持10方节点、亿级求交的业务场景。

（3）高扩展：采用全对称的分布式架构，可随时根据需求增减子节点，满足用户业务快速发展需求。

（4）高互通：以算法模块化、插件化的形式接入不同平台，实现数据、计算的互联互通。

图40 金智塔科技“智隐隐私计算平台”架构图

金智塔科技的“智通数据要素流通平台”综合运用大数据计算、可信环境计算、隐私计算等技术，提供数据产品加工、交付和交易等服务，并对数据产品全生命周期进行安全合规监管，赋能数据产品的市场化流通。产品优势包括：

（1）交付灵活。支持数据包、数据接口、数据报告等标准产品的交付，同时提供个性化数据产品定制；

（2）适配度高。系统能力可插拔，支持交易和交付分离、交易交付合一的模式；

（3）安全性高。平台底层融合了隐私计算和可信环境计算两种技术能力，建立了完善的数据确权、交易、交付监管体系，保证了数据流通安全合规。

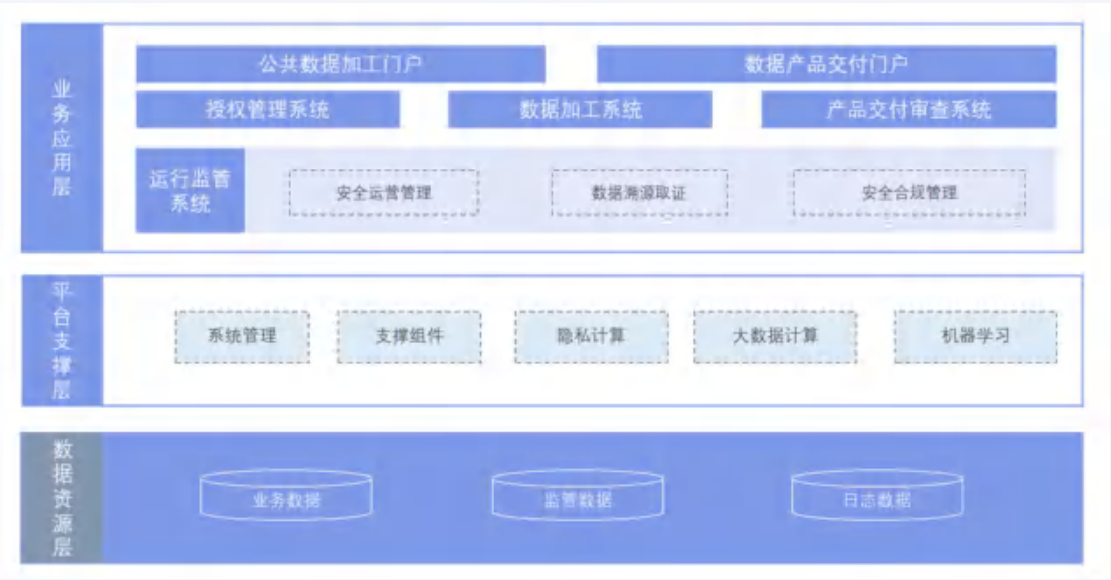


图41 金智塔科技“智通数据要素流通平台”架构图

服务案例

（1）统计微观数据合规多跨共享与创新应用。针对统计基层数据受政策法规约束不能跨部门共享的问题，基于金智塔数据融合计算平台，打破了省统计局与各政府部门间的“数据壁垒”，并安全合规的接入社会数据，构建了省市县三级一体化横向、纵向的统计数据合规应用体系，在保护数据隐私安全的前提下，激发政务数据的应用价值。目前，数据融合计算平台安全合规应用于浙江省统计局、经信厅、征信公司、浙江移动等数据联合计算场景，突破性的实现了统计基层数据安全共享5600万次，已赋能“亩均论英雄联合隐私统计”、“新业态从业人员群体识别和预测”、“双碳数据隐私计算”、等多政府部门的多场景创新应用，助力建设协调高效的数字政府。

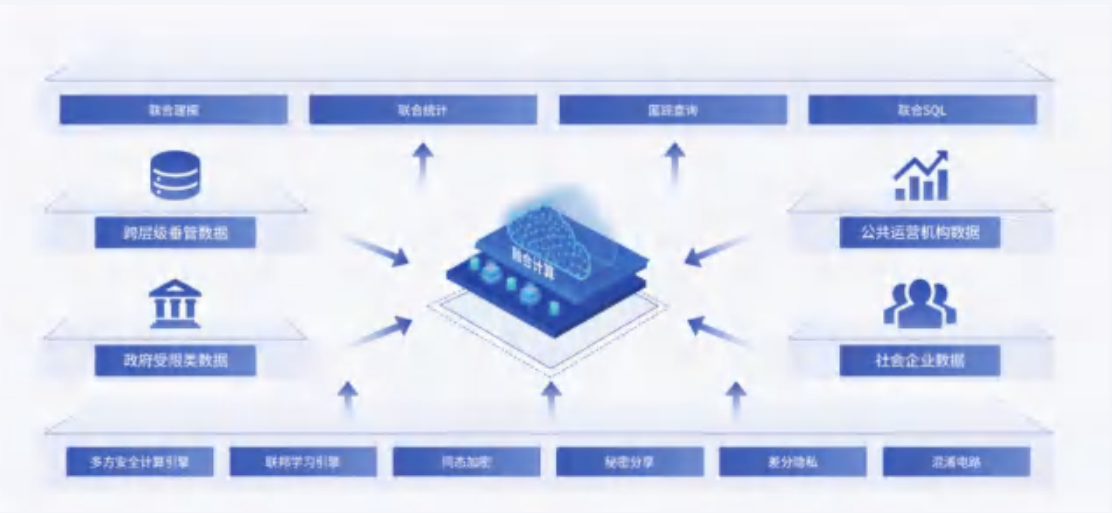


图42 金智塔科技统计数据合规应用场景解决方案

（2）安全融合政府数据赋能小微科创企业授信。针对科创企业由于缺乏数据支持导致融资难的问题，在浙江省地方金融监管局、省银保监的指引下，通过金智塔隐私计算平台安全合规的融合了社会商业数据和公共数据，实现了浙江省金融综合服务平台与浙商银行、浙江农商联合银行等金融机构的联合计算，有效解决某区全域128286家小微企业的在线智能授信问题，科创企业户均授信额度提高63万，企业贷款成本降低50%以上；成功化解了科创企业的融资难、融资贵的难题。

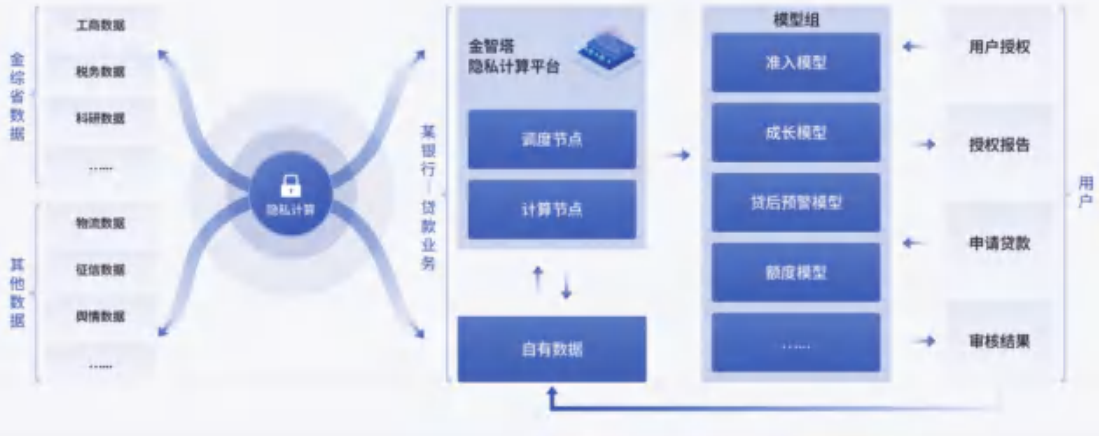


图43金智塔科技小微企业授信融资场景解决方案

（3）合规融合内外部数据助力共同富裕建设。针对个人信息难获取、政务跨部门数据难共享，导致政策投放不精准，共富发展难监测等问题，基于数据流通安全合规底座—金智塔隐私计算平台，融合个人数据、政府数据、市场数据和社会数据，解决政府数据孤岛和个人隐私保护难题，实现数据不出域与可用不可见，设计了家庭幸福指数、发展指数、家庭收入分层、返贫监测等智能模型，对全域三万余户家庭进行监测预警，构建了“数据统计—>需求分析—>群体预警—>举措落实”的工作闭环；并为人民群众智能匹配和自动推送政策，实现了政策和办事智能关联，提升了办事效率，为群众节约50%以上办理时间，较大的提升了某市全域家庭幸福满足感，助力共同富裕示范区高质量建设。

图44 金智塔科技政务数据融合场景解决方案

数据安全产品与服务图谱(2.0)

数据安全通用类产品

数据安全综合类产品

数据安全服务

数据安全推进计划
DATA SECURITY INITIATIVE

简 介

数据安全推进计划（Data Security Initiatives，DSI）是2021年9月1日成立的公益性项目，主要围绕数据安全政策学习、数据安全标准建设、数据安全评估评测、数据安全咨询服务、数据安全人员培训等内容搭建交流平台，构建专业社群。致力于推动法律法规及监管要求的贯彻落实，促进数据安全技术交流，推广数据安全最佳实践，提升数据安全治理水平。

成立至今，DSI成员单位已达300余家，涵盖金融、汽车、互联网、电信、安全厂商等不同行业。并在专家智库、行业工作组、公开课等方面构建专业品牌，输出丰富研究成果。

联系人：姜铎

电　话：13521786562

邮　箱：jiangduo@caict.ac.cn

数据安全推进计划公众号