CSA GCR cloud security alliance
GREATER CHINA REGION ®

数据安全平台神兽方阵报告(2023)

致谢

《数据安全平台神兽方阵报告（2023）》由云安全联盟大中华区组织专家撰写，感谢以下专家的贡献：

主要贡献者：

王安宇　杨天识　艾　龙　许木娣　郭鹏程　姚　凯　邢海韬　潘万鹏　苏泰泉

薛　恺　刘玉红　曹　咪　黄鹏华　江　澎　欧建军

项目评审专家：

李雨航　贾良钰　许木娣　沈　勇　陆琦玮　刘志诚　张　淼　阳志亮　闫新成

吴致远　张　坤　李安伦　石秀金　王　真　朱强炜

研究协调员：

罗智杰

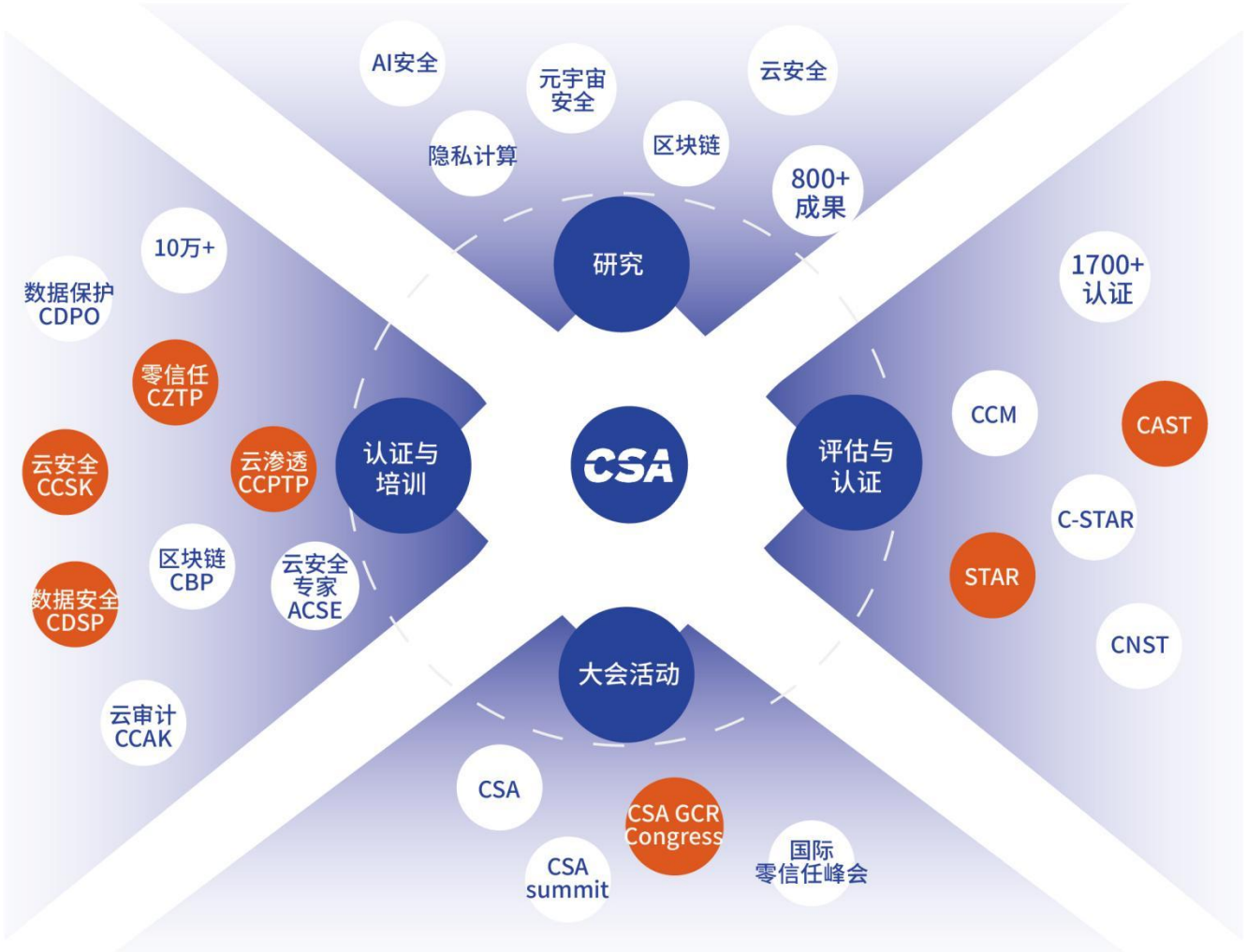
联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

目录

1. 摘要

在第四次工业革命轰轰烈烈地发展了多年后，当今世界已经进入数字经济的时代。它以数字技术为基础，通过数字化的方式改变了经济活动的方式和规模，为经济增长提供了新的动力和机遇，推动了创新和创业的发展。数字经济还改变了产业结构和就业形态，促进了人力资源的优化和社会包容性的提升。同时，数字经济也为可持续发展提供了新的路径和策略，实现了经济增长与环境保护的平衡，对经济发展和社会进步产生了深远的影响。数字技术的发展和应用催生了许多新的商业模式，并衍生出数据价值链的概念，各种新型业务模式通过数字化的连接和交互，实现了资源的优化配置和价值的最大化，推动了数字经济生态系统的建立。

在数字经济时代，数据是最基础也是最关键的生产要素。面对不断变化、飞速演进的数字化世界，要保障数字价值链的安全，必须先保护数据资产的安全。这不仅需要组织做到积极抵御网络安全威胁，增强用户数据隐私，满足行业相关法律法规要求，同时还需要确保数据可在组织内外高效流转，以实现商业价值。有效的解决方案不仅是传统的漏洞扫描、DLP、数据加密、访问控制、身份认证等产品的“集成”或者“集合”，而必须系统化地分析、识别数据的安全风险，有针对性地制定和实施各类安全控制措施，设计和实现安全架构，并持续性地安全运营。这也是“数据安全平台”的主要目标。

2023 年 5 月，国家互联网信息办公室发布的《数字中国发展报告》指出，“2022 年我国数字经济规模达 50.2 万亿元，总量稳居世界第二，同比名义增长 10.3%，占国内生产总值比重提升至 41.5%。2022 年我国网络安全产业规模预计近 2170 亿元，同比增长 13.9%。”随着数字经济快速增长，数据安全保护工作驶入快车道。

在网络安全产业中，数据安全赛道的重视程度逐渐增加，占比也逐渐提升。在数据安全领域，经过调研，在数据安全领域头部云服务厂商，如腾讯云、浪潮云，结合自身云服务安全需求，以及各行业的数字化转型建设经验，对外提供数据安全平台产品。多数综合型网络安全厂商，如上市企业中的天融信、启明星辰、360、安恒信息、绿盟科技，推出了数据安全平台产品和解决方案。一些专业的数据安全厂商，如美创科技，明朝万达等，也结合自己的行业优势，提供数据安全平台产品和解决方案。此外，在数据安全平台领域，还有不少技术驱动的创新企业，将零信任、人工智能等理念或技术用于数据发现、数据治理、风险感知和自适应防护等数据安全平台的基础能力中，并且取得了良好的效果。

云安全联盟大中华区发布《数据安全平台神兽方阵报告（2023）》，从技术领先性、市场影响力等多维度，综合评估各数据安全平台厂商，以帮助读者了解数据安全平台市场趋势，为数据安全平台选型提供借鉴和参考。

2. 神兽方阵报告简介

2.1. 报告介绍

神兽方阵报告是面向数字安全领域的中国企业发展的专业分析报告。通过报告，可以帮助读者了解相关技术及产品的发展情况，并在产业发展中找到适合自己的机会；也可以帮助企业用户了解相关领域各个安全厂商的优势能力，以便更好地进行供应商产品选型。

神兽方阵模型适用数字安全的各个领域。去年，云安全联盟大中华区发布了《中国零信任神兽方阵分析报告（2022 年）》。本报告针对的是数据安全平台领域。未来我们也将发布云安全、AI 安全、物联网安全、隐私科技等领域的报告。

2.2. 神兽方阵模型

神兽方阵（Mythical Creatures Matrix）模型是云安全联盟大中华区基于中国传统文化“神兽”形象创立的分析数字科技企业的数学工具，适用于对数字科技企业在技术、产品成熟度、市场营销及服务等方面的能力与先进性的分析。神兽方阵模型从技术领先性、市场影响力、专家评审、公开路演四个维度评估，在基于企业数据定量分析的基础上，结合各重点行业业务专家和安全专家组成的评审团的谨慎评估，确保评估结果的专业性与公平性。

神兽方阵以“四象”即青龙、白虎、朱雀、玄武为基础。“四象”又称“天之四灵”，分别是中国古典神话中镇守东西南北四方的神兽，其中青龙为东方之神，是四灵之首；朱雀为南方之神，有浴火重生的能力；白虎为西方之神，也是战斗之神；玄武为北方之神，以防守见长。模型的创立旨在为数字安全领域树立具有中国特色科技标杆企业的行业分析品牌。神兽方阵示意图及该模型中各神兽的定位与描述如下：

图 1 神兽方阵模型图

- **青龙神兽企业-综合领先型企业：**在特定领域投入高，且研发能力、产品成熟度、市场营收及知名度等方面的整体实力强的头部企业。

- **朱雀神兽企业－技术深耕型企业：**具备核心竞争力或者技术壁垒，技术研发实力强，产品成熟度高，并且有良好的市场占有率的企业。

- **白虎神兽企业－快速进击型企业：**对市场需求能迅速作出反应，产品的实现与迭代速度快、产品创新能力强，并且市场占有率高的企业。

- **玄武神兽企业-新兴探索型企业：**发展良好的初创企业，或者增加相关领域新业务的传统企业，在技术研发和市场等方面成长迅速，是特定领域快速崛起的生力军，具备强劲的潜力。

2.3. 报告目标

（一）打造符合中国数字安全市场特色的行业评估报告

目前在国际上，对于中国数字安全市场关注度不够，评价数字安全厂商更多基于美国和国际市场，但中国经济体量和互联网应用都处于世界前两位，亟需一个针对中国安全厂商的评价体系。

（二）提供行业趋势洞察与国际对比参考

报告定期更新，反映市场的最新动态和趋势，为企业提供有价值的行业趋势洞察，帮助企业做出更好的战略决策。加强行业共享与协作联动，推动数字安全产业进步。提高与企业高级管理层之间的沟通成效，更好地提升数字安全的商业价值和社会价值。

（三）促进数字安全行业健康发展

数字安全是一个充满挑战，创新驱动，产业边界持续拓宽、飞速发展的行业。无论是行业参与者还是监管者，都应当对数字安全行业的生态发展予以支持，围绕积极的行业价值观，推动数字安全行业的健康发展。

3.数据安全平台产生的背景

3.1. 数据安全的演变历程

随着业务的不断发展，技术的不断进步，数据安全的保护需求和治理理念也经历了多次的变革。从早期主要关注组织内部的数据防护，到如今的全球范围内的数据安全管理，数据安全的演变历程揭示了技术、法规、政策和人类需求间的紧密交织关系。

（一）数据安全 1.0 时代：信息安全中的数据安全

这一阶段的数据安全主要围绕组织内部的数据，重视静态数据防护，针对单一系统如内网数据库和文件共享系统提供保护。核心解决措施包括数据库审计、数据库访问控制和数据防泄露等。

（二）数据安全 2.0 时代：网络安全中的数据安全

随着组织之间的数据交流日益增加，数据安全开始涉及更多的领域和技术。在这个阶段，不仅仅是考虑数据在静态存储下的安全性，还涉及数据在流转与应用中的安全性，因此"Data in Transit"和"Data in Use"的保护变得尤为重要。解决方案包括数据分级分类、综合数据安全平台和 IAM 等。

（三）数据安全 3.0 时代：数字安全中的数据安全

进入新的数字时代，数据的外延进一步扩大，涉及物联网、元宇宙、AI 等前沿技术领域。数据也不再仅仅是企业的资产，更成为国家战略资源。大规模数据流通使得安全风险的影响倍增。此时各组织需要关注的不仅仅是数据保护，同时还需应对全球范围内的隐私保护、确权、交易、跨境等合规问题，满足各国的法规标准。数据安全演进史（见表 1）详细阐述了数据安全从传统防护到现代综合性防护演进的不同阶段。

关键词	数据安全 1.0	数据安全 2.0	数据安全 3.0
概述	信息安全中的数据安全	网络安全中的数据安全	数字安全中的数据安全
场景	单部门单组织多用户数据共享	跨部门跨组织大量用户的数据流通	数据要素市场跨域跨境海量用户的数据交易
环境	内网，数据库、数据仓、文件共享等单系统	互联网，信息共享中心，云数据库，数据湖、大数据平台、数据中台	物联网、元宇宙、AI 等，数据交易所，数据市场，数据工场，数据脱离单独的个人或企业层面成为国家战略资源和核心资产
问题	Data at Rest 静态数据的防护，对数据的访问控制、边界防护、内容审计等	Data in Transit 动态与 Data in Use 使用态数据的防护，对数据进行生命周期的体系化治理	Data Flow 数据流转态的防护，满足国际国家法规标准的数据安全可信体系
产品与解决方案	数据库审计、防火墙、漏洞扫描，DLP 等	数据分级分类，数据安全平台、数据监控与审计、IAM 等	数据治理、控态类、密态类等

表 1 数据安全演进史

随着时间的推进，数据安全的观念从单点技术防护转变为覆盖数据生命周期的整体态势防御，从组织内部的边界防御转向全球数据流通的合规治理。这一演变历程不仅展现了数据安全领域的不断进步，也预示着未来的数据安全将面临更为复杂的挑战和机遇。

3.2. 数据安全面临的挑战

数据安全 3.0 的时代，尤其是在多云、多边界的环境中，数据流动性增强，带来了更多的挑战。行业的主要关注点转向了数据要素流通过程的安全保护。与此同时，国际和国家的法规标准要求构建一个数据安全的可信体系。在全球化的数字时代，数据安全面临以下的主要挑战：

（1）数据资产流转加速，高价值集聚引发更多关注

随着数字化深入，组织拥有的数据资产不再是静态存储，而是在各个主体与场景中不断流动的。数据的高价值集聚和流转，使其成为攻击的主要目标，一旦发生数据安全事件会造成更大且更严重的破坏。如何有效地管理和保护这些数据资产，成为组织亟待解决的问题。

（2）数据处理场景多样，流转态防护复杂化

数据在云端、边缘设备、各类应用间流转，处理活动场景多样化。随之而来的是内外部威胁。在数字化背景下，数据的访问流转、开发利用相比以前更加频繁，数据的暴露面越来越大，相对应的数据面临的安全风险进一步加剧。组织需对数据在流转态的各个节点和阶段进行全面的安全防护。

（3）新技术新应用增加数据流转的复杂性

云计算、大数据、IoT 等新技术的广泛应用，加剧了数据的流转和分散。新的技术环境下，如何确保数据在流转中的安全性，成为一个新的挑战。此外，技术的快速发展意味着安全策略和方法需要不断更新。组织需要保持对新技术的敏感度，并及时调整数据安全策略，应对新技术带来的潜在威胁。

（4）合规压力与数据流转安全相结合

全球范围内的数据保护法规变得越来越严格，如欧盟的 GDPR 和美国的 CCPA 等，我国的《数据安全法》《个人信息保护法》以及各行业领域的条例指引等等，使得组织在处理重要数据和个人敏感信息时必须更加谨慎，并确保数据的合规性。数据在流转态中如何满足这些法规要求，构建一个符合国家和国际标准的数据安全可信体系，是组织必须面对的挑战。

在全球化和数字化双重推动下，数据已经变成了经济增长的关键因素。面对数据安全3.0的挑战，组织亟需对数据安全策略进行不断地创新和升级，以适应日益严格的安全和合规标准。与此同时，广泛的数字化转型推动新兴技术应用以及业务创新，也使得数据超越了传统安全产品的防护范围，数据安全成为未来安全建设的主要抓手，安全产业正驱动新的理念和技术。其中，“数据安全平台（Data Security Platform）”已成为数据安全领域的最新趋势和焦点。

3.3. 数据安全平台的兴起

尽管组织深知数据安全的重要性，但仅仅依赖传统的单一安全产品已经无法满足当前的需求。事实上，为了满足各种合规要求和标准，组织不得不在数据安全上投入大量的资源，但经常面临的问题是资源的重复使用、安全建设周期的延长以及各种安全产品间的互通性问题。这些问题导致了“数据安全孤岛”的出现，即各种安全工具和平台之间无法实现有效的信息共享和合作。

正是看到了这些问题，数据安全平台（DSP）的概念应运而生。与传统的安全产品不同，数据安全平台整合了多种安全技术和工具，为组织提供了一个全面、集中的解决方案。这不仅可以提高数据安全的效率，还可以减少重复的资源投入，确保组织能够更加灵活地应对各种数据安全挑战。

数据安全平台的出现也为组织提供了一个集中、统一和高效的数据保护解决方案，突破了传统安全产品的局限性，使得数据安全管理变得更加简单、直观和有效。此外，随着物联网、AI 和云计算等前沿技术的发展，数据安全平台还能够实时更新，应对新技术带来的潜在风险。

随着数据安全的观念和需求的演变，数据安全平台成为当下和未来数据安全建设的关键。

组织应该尽快认识到这一点，及时调整数据安全策略，确保在全球化和数字化的双重背景下，数据能够得到有效、全面和持续的保护。

4.数据安全平台概述

4.1. 平台的重要性

随着数据逐渐变成新时代生产生活的支柱，数据安全也日益成为保障经济发展、社会稳定和国家安全的重要基石。据最新调查数据显示，2022 年数据安全市场规模为 102 亿，同比增长 15%，而数据安全平台类的产品占比在 15%左右。市场目前具备数据安全平台类产品的企业超过 50 家，具有一定的市场规模和落地应用，且具备较好的发展前景。未来，数据安全技术将持续突破，数据安全在不同行业领域的应用将逐渐深入，预计 2023 年我国数据安全市场规模将达 109.5 亿元。

随着组织机构数据量的不断增加，数据的价值也随之增大，数据应用与流转的需求也在不断增加，面临的数据安全挑战也越来越严峻。现阶段，大多数组织为满足合规检查，需要多种数据安全技术解决数据安全问题。目前，组织在数据安全建设过程中零散部署了各类安全产品，整体方案缺乏体系化，且存在重复建设的情况；另外，各类安全产品之间缺乏有效的联动和统一调度管理，安全风险应对能力难以得到真正提升。

为有效解决当前数据安全保护困境，数据安全建设应当从单一能力向体系化、智能化、融合化转变，将孤立、零散的数据安全保护能力集中到数据安全平台（DSP）中，实现安全能力的统一调度和编排、数据的全生命周期监测、数据安全风险智能识别、数据安全事件联动闭环处置的管控目标。目前，各安全厂商也纷纷开始将各自数据安全能力模块化、原子化，结合平台统一管理的优势，帮助用户从数据安全单点建设走向体系化建设。

4.2. 数据安全平台定义

调研机构 Gartner 在最新发布的《Hype Cycle for Security in China 2022》报告中对该技术的定义是：数据安全平台（Data Security Platforms，简称 DSP）聚合了跨数据类型、存储孤岛和生态系统的数据保护需求，平台应用从数据发现和分类开始，通常通过使用后期绑定访问控制来保护数据，成熟的 DSP 还能进行数据活动监测和执行数据风险评估。

中国信息通信研究院 2021 年主导编制的《电信网和互联网数据安全管控平台技术要求与测试方法》行业标准，正处于报批阶段。标准中将数据安全管控平台定义为具有数据资产管理、敏感数据识别的统一管控能力，能够实现数据安全策略集中化管理、安全事件、安全风险统一管控、集中运维功能，并提供敏感数据分布视图、敏感数据事件视图、敏感数据风险视图和敏感数据策略视图分析展示能力的平台。

从整体上看，数据安全平台的发展正处于起步阶段，国内外各领域、各行业也都在不断探索以数据为中心的平台化综合解决方案。从合规遵循、业务发展、风险防控等多方面需求来看，平台化的解决方案是解决当前复杂环境下数据安全治理问题的必经之路。

综上，我们认为数据安全平台（DSP）是一个全面的集成系统，能够提供数据资产管理、数据安全风险监测与预警、数据安全策略管控、数据安全审计监督，以及数据安全运营等关键功能，融合了机器学习、智能流程编排和隐私计算等众多先进技术，并能实现对数据资产识别、数据分类分级、数据访问控制、数据加密、数据脱敏、数据水印、数据审计、数据泄露防护等多种数据安全能力组件的集中联动和管控，确保数据在全生命周期中受保护以及保障数据处理的合法合规。同时，数据安全平台（DSP）展现出极高的灵活性和扩展性，适应于不同环境下的多样化数据安全需求。

4.3. 数据安全平台介绍

4.3.1. 数据安全平台演变

从数据安全 1.0 时代至今，我们可以看到安全能力的不断演变和增强。如今，大多数的数据安全平台都包括了一些核心能力（下图蓝色标注）。随着技术的进步，这些平台还在不断优化，减少安全能力之间的差距并提高数据安全策略的精细化。

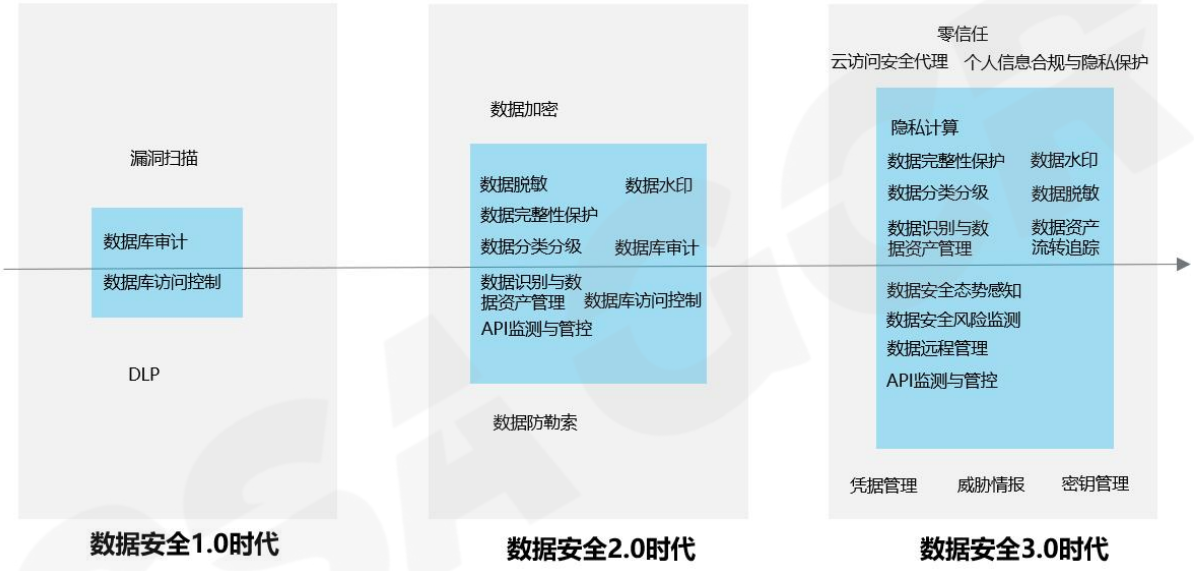


图 2 数据安全平台能力演变进程

在产品开发的层面，数据安全产品的设计与扩展往往围绕其核心技术能力展开。一类平台产品初期主要关注数据内容保护技术。但随着时间的推移，它们进一步扩充功能，引入数据库活动监控、数据水印以及数据脱敏技术。另一类产品以访问控制为切入点，利用动态数据脱敏网关技术重构审计日志，从而增强对数据库的实时监控审计、数据分类分级，并逐步涉及更广泛的数据安全治理领域。

此外，公有云厂商为用户构建了一套公有云原生的数据安全治理框架，依赖于云服务的

弹性和可伸缩性，以提供连续的数据保护、加密存储和访问控制等能力。密码服务厂商主要关注数据的加密和解密技术，提供多种加密算法和策略来确保数据的机密性和完整性。

数据安全平台从最开始的以数据库审计和访问控制的简单集中管理方案演变为目前的一个数据安全管控和运营的生态体系。未来数据安全平台将集成更多安全能力，通过安全平台和安全能力单元的联动联防，集成更多的数据安全能力并支持下发安全策略，从而实现数据安全持续运营的目标。

4.3.2. 数据安全平台能力组件

根据本次调研显示，众多数据安全厂商正将其现有的产品功能整合到统一的数据安全平台上。这些平台能够提供诸如数据资产发现、数据脱敏、数据库审计、数据分类分级、云端数据活动监控、数据加密等安全能力。这种整合使得以前分散的安全防护产品在一个统一平台上得到融合，确保数据安全平台在整个数据安全建设中发挥核心作用。**数据安全平台所具备的重要安全能力：**

- **数据识别：**这一能力涉及识别、分类和管理组织内所有的数据资产。通过自动或半自动的方式，它可以发现敏感数据、私有数据或企业关键数据，并根据其价值和敏感性进行分类和标记。

- **数据分类分级：**这是一个系统的对数据进行分类和分级的过程，通常基于数据的敏感性、重要性和业务价值。数据可以被标记为公开的、内部的、机密的等等。

- **数据安全风险监测：**这一功能通过持续监控和分析数据活动，识别异常行为或潜在的安全威胁，及时发现和响应数据安全事件，从而减少数据泄露或损坏的风险。

- **数据安全态势感知：**这是一个集成的视图，展示组织的整体数据安全状况。它通过

收集、分析和可视化来自各种源的安全数据来实现。使安全团队能够更快速、更有效地识别和应对安全威胁，同时为组织的高层管理提供有关数据安全健康状况的实时洞察。

- **数据安全策略管控：**通过与数据安全风险监测能力的联动，实现及时响应数据安全风险，快速调度各类数据安全能力组件实施数据安全保护的主要能力，并能够将各类数据安全能力组件的状态和配置进行统一的管理和运营。

4.3.3. 数据安全平台的技术路线

根据本次调研显示，数据安全平台通过集成多种技术和策略，提供了一个全方位的安全管理解决方案，用于应对复杂的数据安全挑战。下图是当前数据安全平台实现的关键技术路线：

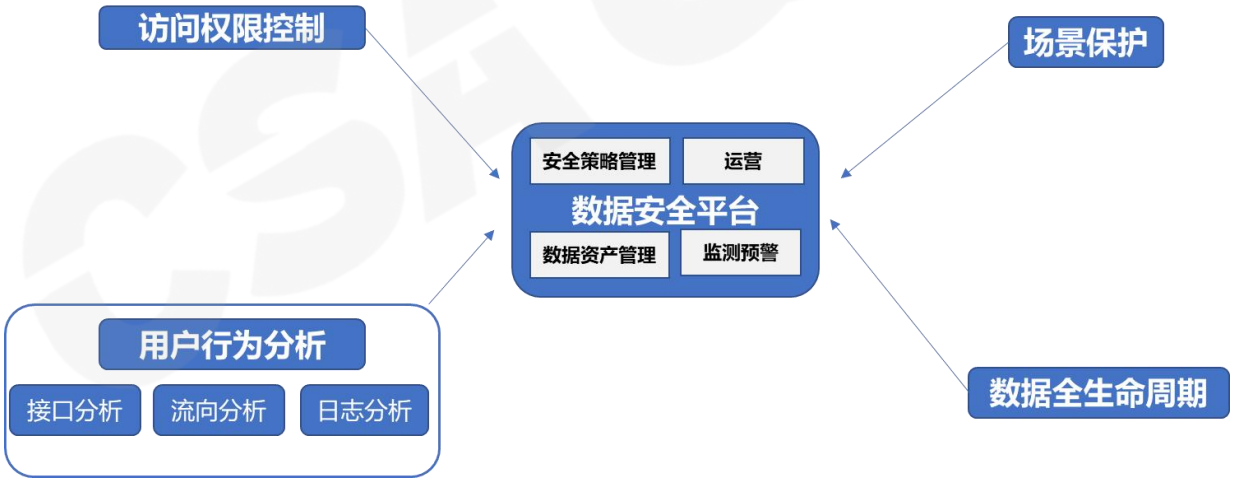


图 3 数据安全平台实现的关键技术路线图

（一）基于数据权限的访问控制

平台利用细致的权限管理策略来控制用户对数据的访问。这种控制基于用户的身份、角色以及与数据相关的策略，通过实行严格的密码策略、多因素认证和基于角色的访问控

制系统，确保只有合适的权限被授予相应的用户。这不仅限于验证用户身份，还包括为每类用户分配正确的数据操作权限，如读取、修改、删除等。

（二）基于数据全生命周期的管理

平台跟踪和保护数据的每一个生命周期阶段，从创建、存储、使用到最终的销毁。这包括数据的加密、脱敏以及定期的安全审计，确保数据在其整个生命周期中的保密性、完整性和可用性。

（三）基于场景化的管理

平台支持基于特定业务场景的安全策略定制，从云环境到移动平台，再到端到端的数据交换，在充分理解不同业务场景安全偏好的基础上，平衡每一种场景下数据安全保护和开发利用。

（四）基于用户行为分析的数据安全

侧重于通过监控和分析用户对数据的操作行为来提高安全性。利用行为分析技术，系统能够识别出异常行为模式，从而及时发现内部威胁或外部攻击的迹象。

每项技术路线的实施都需综合考虑技术成熟度、业务需求、用户体验和安全性之间的平衡。数据安全平台应持续适应新兴的安全威胁和业务模式的演变，确保提供符合当前市场需求的解决方案。

5. 数据安全神兽方阵

5.1. 2023 数据安全平台神兽方阵

云安全联盟大中华区综合考虑了企业的技术领先性、市场影响力等因素，分别对应各神兽方阵数据模型的入选标准，筛选出一批在数据安全平台领域内具有一定规模，在业界有一定知名度和影响力，或者处于起步阶段但技术实力强和快速成长阶段的企业，作为2023 年数据安全平台领域的神兽企业。本次共 22 家，其中青龙神兽企业 4 家，朱雀神兽企业 7 家，白虎神兽企业 5 家，玄武神兽企业 6 家。

图 4 2023 数据安全平台神兽方阵

- **青龙神兽企业-综合领先型企业：**北京启明星辰信息安全技术有限公司、上海观安信息技术股份有限公司、天融信科技集团股份有限公司、腾讯云计算（北京）有限责任公司（4 家）

- **朱雀神兽企业-技术深耕型企业：**北京神州绿盟科技有限公司、北京明朝万达科技股份有限公司、杭州美创科技股份有限公司、杭州安恒信息技术股份有限公司、深圳市联软科技股份有限公司、三六零数字安全科技集团有限公司、亚信安全科技股份有限公司（7 家）

- **白虎神兽企业-快速进击型企业：**杭州世平信息科技有限公司、江苏保旺达软件技术有限公司、浪潮云信息技术股份公司、三未信安科技股份有限公司、厦门服云信息科技有限公司（5 家）

- **玄武神兽企业-新兴探索型企业：**北京数安行科技有限公司、北京从云科技有限公司、杭州亿格云科技有限公司、杭州虎符网络有限公司、数篷科技（深圳）有限公司、上海安几科技有限公司（6 家）

5.2. 入选企业及产品/平台的介绍

5.2.1. 北京启明星辰信息安全技术有限公司

（一）简介

启明星辰集团自 2000 年自主研发出第一款硬件 IDS 产品——天阗入侵检测系统后，持续发力网络安全硬件市场，陆续发布 IPS、UTM、WAF、VPN、堡垒机等多款产品，形成了完整的网络安全硬件产品生态体系，深度赋能政府、运营商、金融、税务、能源、交通、制造等多个行业领域，备受用户的高度认可与青睐。

（二）点评

启明星辰集团在中国网络安全硬件市场名列前茅，其数据安全治理管控平台通过敏感数据的发现和有效管理，确保业务数据的保密性；通过数据安全确权、审计及数据安全使用管理，确保数据的可用性；通过全面的数据安全防护、校验检查及相应的管理措施，确保数据的完整性。案例实现了数据全生命周期管控，在大数据局、移动、电信、联通等运营商均有应用。

5.2.2. 上海观安信息技术股份有限公司

（一）简介

观安信息在数据安全领域作为标准制定者与技术引领者，推进了数据安全领域发展。观安参与制定了数个国家级标准，如数据安全能力成熟度标准，数据敏感标准等。在技术方面，观安信息首次提出并产品化数据安全扫描器技术及数据流转探针技术，并在大型企业落地实施。在产品方面，观安围绕核心技术构建起敏感数据发现及分类分级、数据脱敏、数据水印、数据流转及风险监测、API 管控、数据库审计、数据安全管控平台等多款产品，并在部分市场得到占有率第一的位置，并已大量服务于全行业客户。

（二）点评

观安信息通过静态主动扫描和动态流量发现结合的手段进行数据资产梳理。通过多维度指标判定引擎识别数据特征，提升发现和识别的精准度。通过多级管线处理技术，提高流转行为分析和风险精准度。基于全链路、多层关联的审计要素机制，实现高效事件定位定责。观安信息大量服务于全行业客户，是专业数据安全实践者。

5.2.3. 天融信科技集团股份有限公司

（一）简介

天融信在数据安全领域深耕多年，积累了丰富的数据安全管理经验，提出“以数据为中心的安全建设体系”的建设思路，形成了一套“以数据安全治理为基础、数据安全全生命周期监管、数据安全技术手段防护”的数据全生命周期的解决方案，为客户打造具备识别、防护、检测、响应、恢复闭环能力为一体的纵深数据安全防御体系，提供了多款数据安全类产品及服务。

（二）点评

天融信长期深耕安全领域，以数据安全管理平台为核心，以数据安全防护为手段，数据安全生命周期为管理核心，数据安全服务为支撑，为客户提供了体系化的数据安全管理能力，能实现数据资产全面识别与统一管理、快速定级与备案管理、组件备案与精准防护、风险发现与监测告警，实现全面合规、协同智能、统一集中的数据安全管控；同时在数据风险视图方面提供了比较好的支撑能力，满足企业的数据安全管控要求。产品广泛应用于政府、运营商、能源、金融等多个行业。

5.2.4. 腾讯云计算（北京）有限责任公司

（一）简介

腾讯安全致力于成为产业数字化升级进程中的安全战略官，依托 20 年多业务安全运营及黑灰产对抗经验，凭借行业顶尖安全专家、最完备安全大数据及 AI 技术积累，依托 7 大安全实验室，为企业从“情报－攻防－管理－规划”四维构建安全战略，并提供紧贴业务需要的安全最佳实践，守护政府及企业的数据、系统、业务安全，为产业数字化升级保驾护航。数据安全业务作为腾讯云鼎实验室的核心业务，产品层面从业内前沿技术研究和内部数据治理经验方面都得到了众多资源支持，进而孵化出商业化产品，为各大

政企客户提供优秀的数据安全能力。

（二）点评

腾讯云在云安全防护和治理、云原生安全技术、密码学和云数据安全、容器和虚拟化安全、硬固件和基础设施安全等多个领域展开技术研究和产品创新工作，保障云平台及云上数百万租户的安全，为各大政企客户提供优秀的数据安全能力。

5.2.5. 北京神州绿盟科技有限公司

（一）简介

绿盟科技于 2004 年成立，经历二十多年的发展，已成为国内领先的综合性网络安全公司。公司历来重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域积极探索，为公司的核心竞争力的持续提升提供了有力保障。

（二）点评

绿盟科技向客户提供全品类网络安全产品，场景化安全解决方案，以及各类安全服务、运营服务等。绿盟数据安全运营平台是以数据安全合规为目标、数据资产为核心、持续检测数据安全风险的平台产品，该平台汇聚全网数据安全日志，内置多种数据安全场景和分析模型，呈现全网数据安全综合态势，能够帮助用户体系化建设数据安全能力，提升数据安全效率，为客户提供“一站式”产品和解决方案。

5.2.6. 北京明朝万达科技股份有限公司

（一）简介

北京明朝万达科技股份有限公司成立于 2005 年，是中国新一代信息安全技术企业的代表厂商，专注于数据安全、公共安全、云安全、大数据安全及加密应用技术解决方案等服务。明朝万达以数据安全为核心、自主可控的国密算法应用技术为基础，研发的 Chinasec（安元）数据安全系列产品及解决方案，覆盖数据产生、存储、交换、使用等全生命周期重要环节，实现对服务器、数据库、PC 终端、移动终端以及网络通信的全 IT 架构下数据安全的协同联动管理，打造企业级的数据安全防护体系。

（二）点评

明朝万达以数据安全为核心，产品覆盖全面，数据保护、网络数据安全、云数据安全均有涉猎。其中数据保护产品覆盖数据安全管理系统，数据安全 SDK、数据安全保镖、数据安全保险箱、数据安全合规检测工具等，网络数据安全保护产品包含数据防泄漏系统、安全接入网关系统、数据安全交换系统、视频安全交换系统、网页防篡改系统等，云数据安全保护产品包含云访问安全代理系统、微服务应用支撑系统、安全集中监控与审计系统、互联网数据泄漏检测系统等。明朝万达的产品覆盖数据全生命周期，囊括数据治理与防御，应用场景广泛。

5.2.7. 杭州安恒信息技术股份有限公司

（一）简介

安恒信息主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。凭借强大的研发实力和持续的产品创新，公司已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全平台以及网络信息安全服务，各产品线及业务线在行业中均形成了强大的竞争力。

（二）点评

安恒信息数据安全管控平台提供安全数据的采集和汇聚服务，数据清洗和预处理服务，并从体系化角度出发，以风险控制各个阶段为抓手，建立数据安全运营平台，通过归集基础设施、数据资源、应用支撑、业务应用的安全日志及情报数据，汇总安全运营中产生的安全威胁数据，打破“信息孤岛、数据烟囱”等现象，建立统一的数据中心，通过数据治理、分析和安全场景建模，实现安全风险的分析、监控、预警、处置等。

5.2.8. 杭州美创科技股份有限公司

（一）简介

美创科技拥有自主研发的全系列数据安全产品，能结合行业数据安全监管要求及业务特点，为政府、金融、能源、医疗、物流交通等行业客户提供行业数据安全整体解决方案。美创推出的新一代数据安全管理平台是面向多云环境提供复杂数据资产安全管理、数据流动安全管控、数据安全风险监测的管控平台，能够实现多层级防护机制的构建。

（二）点评

美创新一代数据安全管理平台，贯彻了“以资产为中心，以身份为边界，以风险为界面”的核心理念，在统一的云中心收敛安全业务差异性，实现全域的资产治理、身份治理、风险治理，实现业务逻辑复杂性管理；同时，在端侧以轻量级端点智能控制为核心，快速匹配场景；通过适应性进化和持续迭代，持续保障身份和资产全生命周期的安全。

5.2.9. 深圳市联软科技股份有限公司

（一）简介

联软科技股份有限公司持续专注于企业级网络安全市场，以覆盖云、边、端等多场景的平台级网络安全解决方案为核心，围绕端点安全、边界安全和云安全，为政企客户提供网络安全产品和服务。联软聚焦防泄密、防勒索(入侵)、全网零信任三大核心赛道，为政企客户数字化转型筑牢安全防线。能够为企业带来安全与效率的平衡，确保终端数据安全管控的有效落地。

（二）点评

联软科技长期深耕企业级网络安全管控领域，以覆盖云、边、端多场景的端点安全管控为核心拓展数据安全保护。以办公终端数据防泄密解决方案为核心，通过对不同业务场景的梳理，形成了网络边界保护、终端保护、数据保护及主动防御等安全组件，整合了DLP、终端准入管理、重要数据加密、外发授权等方式，基于场景化方案，按数据生命周期的相关过程，实现数据安全的全面掌控。产品在政府、金融、医疗和高端制造等行业有成功应用案例。

5.2.10. 三六零数字安全科技集团有限公司

（一）简介

360 数据安全管理平台产品是对各类数据安全能力进行一个内聚的、闭环的整合，其整合思想的本质是数据安全层面的 XDR。与传统的 XDR 概念不同的是，这是一个垂直领域的 XDR。打破原有的独立数据安全产品边界，根据数据安全监测、防护和运营的需求，提供各种核心能力组件，进行统一的一体化解决方案设计。产品主要由数据安全管理平台、数据分类分级探针、数据库审计、数据库防火墙、静态脱敏、动态脱敏、数据资产发现、零信任、数据防泄漏、安全桌面、堡垒机、终端管控、多种溯源取证等构成全方位数据安全解决方案。

（二）点评

360 数据安全管理平台通过对数据安全日志、流量等的采集和深度关联分析，发现敏感数据的位置分布、分类分级态势、流转态势、风险态势、使用态势、合规态势，向政企等机构提供真正端到端全链路、全方位分析视图，帮助政企等机构及时发现数据安全风险，满足合规建设要求。

5.2.11. 亚信安全科技股份有限公司

（一）简介

亚信安全是中国网络安全软件领域的领跑者，是业内“懂网、懂云”的网络安全公司。亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理及 5G 安全等领域突破核心技术，用实力筑牢云、网、边、端之安全防线。

（二）点评

亚信安全的信数数据安全治理平台从数据资产、安全策略、风险监视三个方向上，实现了数据安全的运营、数据安全策略管理、安全风险监测和安全风险处置功能。在打造亚信安全数据能力生态的基础上，以场景化的联动方案帮助客户完成数据安全治理的具体落地。其平台支持上百种数据源接入，能灵活适配异构数据源类型，综合分析及联动处置能力有效避免数据孤岛。具备市场发展优势。

5.2.12. 杭州世平信息科技有限公司

（一）简介

世平信息在数据内容识别和数据安全合规领域深耕多年，持续进行法律法规解读、前瞻

技术的开拓性研发，形成专业、领先的数据安全产品、平台与服务体系，为用户提供数据资产/敏感数据发现、数据分类分级与管理、数据安全合规性风险检测评估与监管，以及基于业务流程的精细化数据安全管控等业界前沿能力。产品与解决方案可实现针对涉密数据、个人信息和重要数据的合规性与内源性数据安全风险的识别管控，满足监管部门、政企用户的数据安全治理需求。

（二）点评

作为一家深耕数据安全领域的公司，世平信息为企业客户提供了从数据内容安全、数据库安全到数据安全管理、数据安全防护、数据安全合规管理等一系列的安全解决方案，通过“内容+合规”的方式进行数据安全的合规风险评估和管理，能建立全面的、贴合业务的数据安全治理体系。产品在金融、国土、保密、教育、制造行业都有成功的应用案例。

5.2.13. 江苏保旺达软件技术有限公司

（一）简介

保旺达成立于 2011 年，始终专注于数据安全领域的创新实践，不断推出全新理念、前沿技术与创新型产品，是专业数据安全实践者。保旺达的数据安全运营管理平台、数据分级分类、数字支持扫描发现、文档安全和数据安全网关等重点产品结合相关业务领域的特点，能够为客户提供安全、合规、全生命周期、全业务场景的网络安全整体解决方案和服务，为企业数字化转型提供数字安全保障。

（二）点评

保旺达作为专业数据安全的实践者，建立的数据安全运营管理平台，通过整合自身的众多数据安全产品，通过 SATE（定规范、摸家底、强管控、重运营）方法开展数据的安

全治理，以合规为引导，识别需保护的资产，加强流程管控，实现职责和治理的落地。保旺达构建了合规和安全的双驱动数据安全整体防护体系，为客户构建了一整套的全面、合规、智慧化的数据安全管控解决方案。产品在政府、运营商、军工、金融、能源等行业有成功的应用案例。

5.2.14. 浪潮云信息技术股份公司

（一）简介

浪潮云是中国最早提供云服务的厂商之一（2010），是首批国家机关云服务提供商。作为中国分布式云的引领者，浪潮云致力于成为高品质云服务提供商，具备“专业、生态、可信赖”三大核心优势。浪潮云始终坚持以客户为中心，以满足客户需求为驱动，积极投入研发资源，致力于在云计算、大数据、人工智能等领域探索和开发最新的技术，持续不断地投入资源进行研发，保持技术领先地位。

（二）点评

浪潮云以广泛的市场渠道和客户基础，打造数据安全管理体系、数据技术安全体系、数据运营安全体系。通过浪潮云数据安全综合解决方案，能实现基础安全和数据全生命周期安全能力等级评估，促进组织机构了解并提升自身的数据安全水平，量化数据安全能力内容并明确安全建设规划。从专业体系化角度，协助政企用户高效、高质量地通过DSMM 评估。浪潮云具备“专业、生态、可信赖”三大核心优势，并具备核心市场竞争力。

5.2.15. 三未信安科技股份有限公司

（一）简介

三未信安是一家专注于信息安全领域的高科技企业，成立于 2002 年，有丰富的安全产品和服务，尤其在信创方面，具备完整密码产品体系和信创密码建设能力，并将这些能力应用到云计算、大数据、物联网、车联网、人工智能、区块链、隐私保护计算等新兴技术领域。数据安全平台解决方案以密码服务平台为承载，以密钥管理系统为核心，通过硬件安全模块的保护，实现密钥管理和密码运算功能，能够为应用、数据库、文件系统以及大数据解决方案的安全管控提供细粒度的访问控制，以及静态数据的保护方案。

（二）点评

三未信安在密码技术有深厚的积累，以密码技术的创新应用为突破口，结合密码服务和数据安全管理的技术，实现数据流转中的安全管控。通过企业级的密钥管理生态，结合应用、数据库、大数据平台、数据存储、云应用等场景提供了数据安全管控方面的新思路和新角度，可以实现基于密钥管控的细粒度访问控制。产品广泛应用于金融、证券、能源、电信、交通、电子商务等行业，以及海关、公安、税务、水利、质量监督、医疗保障等政府部门。

5.2.16. 厦门服云信息科技有限公司

（一）简介

厦门服云信息科技有限公司（品牌名：安全狗）成立于 2013 年，致力于提供云安全领域相关产品、服务及解决方案，是国内最早引入云工作负载安全（CWPP）概念，并成功构建相应产品线的专业云安全厂商。目前拥有数十项产品专利及著作权证书，产品能力获得信通院、公安三所、Gartner、CSA、IDC 等多个国内外权威机构的认可。

（二）点评

安全狗以网络安全为基础，通过建立数据全程的数据安全保障技术体系以及安全服务运营体系，并制定完善的数据安全管理制度，从根本上保障了企业数据安全建设。其数据安全集中管控平台实现全数据资产测绘、全数据统一管控，全数据路径分析，数据流向三层溯源，数据风险全栈溯源，帮助用户有效预测风险、精准感知威胁、提升响应效率。

5.2.17. 北京数安行科技有限公司

（一）简介

数安行是一家专注于数据运营安全的创新型数据安全厂商。主营产品涵盖数据分类分级，数据安全风险监测评估，数据安全风险态势感知，个人信息合规与隐私保护，数据安全计算与计量，零信任数据安全防护、数据运营安全等，主要为数字化背景的企业提供数据安全产品和服务。公司以 DataSecOps 为理念，以 AI 人工智能技术为核心驱动，致力于让用户的数据安全地创造价值。公司核心团队拥有近 20 年网络安全与数据安全经验，技术积累雄厚，服务于金融、运营商、互联网、教育、高端制造、软件与信息技术服务、工业互联网、能源等各行业客户。

（二）点评

数安行数据安全风险监测响应系统，以 DataSecOps 框架为理念，融合 AI 人工智能，智能监测数据处理活动，涵盖数据的收集、存储、使用、加工、传输、提供、公开等活动，对数据安全风险进行探测与智能评估，在合规性方面具有良好的适应性，在工业互联网领域的验证效果显著。同时，也适应于政务、 金融、运营商、软件与信息化领域、高端制造、能源等各行业的数据安全风险的监测以及数据的安全防护，在市场发展方面有较好的增长性。

5.2.18. 北京从云科技有限公司

（一）简介

从云科技成立于 2018 年，是一家数据安全产品方案和服务提供商。其建立的数据安全平台聚焦业务数据流转的全流程保护，保障业务访问安全。方案基于 AODS（Aspect Oriented Data Security，数据安全切面），以业务融合、技术解耦的思路，践行并落地数据安全能力原生化，为客户提供数据安全体系化建设服务。通过此方案，可在业务零改造的情况下，聚焦业务数据本身，为业务数据流转的各个关键节点构建多维度、多层次解耦的数据安全切面，实现业务数据访问的私有、高效、安全和智慧，实现业务数据全流程的深度识别、智能控制和可视化追踪。

（二）点评

从云科技作为数据安全领域的新兴创业公司，通过构建数据安全能力原生化，分析业务数据流转的安全需求，以 7 个关键产品组件对数据流转安全进行统一的编排和保护，实现数据在不同场景下的安全管控。产品支持云和私有化部署的方式，可以为不同需求的客户提供数据安全保护。产品在金融、政府、互联网、生物制药、教育等行业有成功应用的案例。

5.2.19. 杭州亿格云科技有限公司

（一）简介

亿格云成立于 2021 年 7 月，亿格云是一家 SASE 安全服务商，通过自主研发的 SASE 服务平台—亿格云枢，产品提供包括零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）和统一端点管理（UEM）等功能，帮助企业以更低成本、更高效率，建设更加安全、更好体验的下一代办公场景的安全体系，从而解决企业数字化转型过程中遇到的混合和分支办公安全、数据安全、

终端安全等问题。

（二）点评

作为数据安全领域的新兴创业公司，亿格云为企业客户提供基于零信任的 XDLP 数据安全解决方案，该方案能够提供从数据下载到流转到外发的全链路跟踪，通过对业务上下文的识别，在全场景应用 DLP 技术进行全域风险评估，其优势在于能够全方位、全场景地覆盖数据生命周期。产品在智能制造、金融、游戏、泛互联网等行业有成功的应用案例。

5.2.20. 杭州虎符网络有限公司

（一）简介

基于“聚焦零信任安全，构建身份网络，重塑办公安全”的产品理念，虎符网络推出虎影零信任数据访问安全产品，通过云数据沙箱技术解决数据安全共享、访问及使用的问题，帮助用户以轻量化、非侵入式方式实现内部数据的安全访问和流转管控，促进企业数字化安全转型，目前已成功运用于互联网、电子政务、运营商、环保、金融等行业头部客户。

（二）点评

虎符网络的虎影数据访问安全系统基于虚拟投影技术，将应用执行和显示分离，确保数据所有权和使用权分离，打造新一代数据安全管控和隔离方案，实现数据传输、使用、共享安全。构建虚拟数据资源安全边界，实现数据流转全流程管控。解决大数据管理局外部远程运维和驻场开发需求，可持续优化拓展。

5.2.21. 数篷科技 (深圳)有限公司

（一）简介

数篷科技是面向数据的网络安全架构创新公司，成立于 2018 年，长期致力于数据安全平台的研发，拥有较强且综合的竞争实力。从产品层面看，数篷科技基于“安全即基础设施”理念，推出了企业安全工作空间 DACS Pro、企业数据访问控制系统 DACS Lite 和企业移动安全工作空间 DACS Mobile，是国内领先的数据安全解决方案，能够帮助企业快速完成数字化转型及云时代所需的基础架构升级。

（二）点评

数篷科技作为一家提供数据安全平台及解决方案的技术创新型企业，在数据安全保护方面，采用了新一代安全沙箱、软件定义边界、AI 安全策略等多项前沿技术实现对敏感数据的精确访问控制及有效隔离管控，适用的主要场景包括：研发代码保护、外包人员安全管控、数据分级管理、大数据分析等。结合企业数据访问控制系统和企业移动安全空间，能够实现更细粒度的安全管控，为企业应对大数据时代的复杂需求提供帮助。产品在保险、游戏、电商、金融、高端制造行业有成功的应用案例。

5.2.22. 上海安几科技有限公司

（一）简介

安几网安创立于 2018 年，组建了由一流的数据安全专家和工程师组成的研发团队，以零信任理念，搭建了专业的数据管理和安全保护工具：数据安全管控平台。平台包含了数据资产梳理、数据分类分级、数据生命周期管理、数据运营监测、数据授权流动监控等底座功能，能够提供全面的数据管理能力和细粒度的权限控制，并具有数据流动与访

问路径的可视化能力，提供了能够满足不同企业需求的数据安全管控解决方案。

（二）点评

安几网安以“零信任+沙盒+人工智能”等为核心技术，构建了适用于员工远程访问高敏数据、多分支机构远程访问、运维、移动办公以及大数据中心安全访问场景的数据安全管控平台。通过构建全面的数据管理能力，在帮助企业全面了解和管理企业数据资产的同时，对数据进行了细粒度的权限控制；同时还能够根据不同的合规要求，自动调整数据的管理操作，能够帮助客户满足合规性要求，减少合规风险；同时还能够对数据的流动和访问路径进行可视化的管理，实现数据监测的实时性以及预警管控。产品在政府、金融、高端制造、生物医疗、零售等行业有成功应用案例。

6.分析与总结

6.1. 主要发现和结论

（一）重点技术应用

根据本次调研显示，使用了 AI 技术的数据安全平台占有 62%，使用了机器学习技术的占 35%，使用了隐私计算技术的占 25%，其他选项例如自然语言处理（NLP）、加密技术、区块链、零信任等共计 45%。其中，部分产品综合运用了多种重点技术。根据以上的分析，可以看出数据安全产品在新技术应用方面呈现出以下几个动态：

- **AI 技术应用增长：**调研结果显示 AI 技术是所有重点技术中应用最广泛的，这表明 AI 技术在数据安全产品中的应用呈增长趋势。AI 技术能够对大量的数据分析和处理，提高数据安全的效果和准确性。数据安全产品厂商越来越意识到 AI 技术的潜力，并将其纳入产品中以提升安全性能。

- **机器学习广泛应用：**机器学习作为 AI 技术的重要分支，在数据安全产品中得到广泛应用。通过训练算法和模型，机器学习使计算机能够通过数据学习和改进，提高数据安全的能力。这表明数据安全产品厂商越来越重视机器学习技术的应用，增强了产品的智能化和自适应性。

- **隐私计算的兴起：**隐私计算可以在不暴露原始数据的前提下计算和分析，解决数据流通、数据应用等数据服务问题。隐私计算在数据安全产品中的应用也在逐渐兴起，数据安全产品厂商越来越注重用户数据的保密性，隐私计算提供了一种有效的解决方案。

- **多样化技术应用：**除了 AI 技术、机器学习和隐私计算，多名受访者表示他们的产

品运用了多种新型技术，这表明数据安全产品领域对于多样化技术的应用有一定的需求。厂商和组织在努力探索和应用不同的技术手段，以满足不同用户的需求和应对不同的安全挑战。

综上所述，数据安全产品在新技术应用方面呈现出高速增长、广泛应用、场景丰富多样的趋势。这些趋势反映了数据安全业务场景对创新技术的需求，并促使相关企业和组织在产品开发和解决方案设计中不断探索和采用新的技术。

（二）待提升的地方

根据本次调研显示，对于新技术应用所针对的重要功能模块集中在数据识别、分类分级、访问控制、审计、风险监测与处置等，这些功能模块与数据生命周期治理活动密切相关，旨在确保数据的安全和合规性。

值得注意的是，尽管受访厂家对于技术应用的表述比较明确，但对于新技术应用后所能提升的功能描述则比较模糊。除了上述数据识别、分类分级等典型的数据生命周期治理活动外，对平台功能提升的描述经常会使用“数据保护”“管理”“运营”“数据要素全流通”等空泛的用语，缺乏具体的细节和实际效益的说明。这可能说明几个问题：

- **缺乏具体案例和实际效益的证明：**厂家在描述新技术应用后的功能提升时，可能缺乏具体的案例和实际效益的说明。他们可能更关注技术本身的特点和能力，而对于如何将这些技术应用到实际场景中，以实现具体的功能提升，缺乏深入的阐述。

- **技术落地和应用的挑战：**新技术的应用和落地往往面临一些挑战，包括技术成熟度、资源投入、组织变革等方面。受访厂家可能意识到这些挑战存在，因此在描述功能提升时使用了较为宽泛的用语，以避免过于具体的承诺或过高的期望。

- **客户需求多样化：**不同的客户对于数据安全产品的需求和关注点可能存在差异。受

访厂家可能使用较为宽泛的描述，涵盖不同客户的需求。同时，由于数据安全产品涉及的领域广泛，功能提升也可能是一项复杂的任务，涉及多个方面的技术和功能，因此在描述时可能更倾向于使用泛化的表述。

在选择和采购数据安全产品时，用户单位可能需要进一步与厂家沟通，以了解具体的功能和实际效益。

（三）平台的主要应用场景

根据本次调研显示，数据安全平台主要应用场景中，云计算占 26%、工业互联网占 19%、车联网和智慧场景均占 16%，物联网占 13%，其他场景占 10%。大部分平台产品适用于多种场景。这说明以下几点：

- **多样化的应用场景需求：**不同的行业和领域在数据安全方面的需求各不相同。数据安全平台产品厂商意识到这一点，并根据不同的应用场景对数据安全能力进行规划。云计算、工业互联网、车联网、智慧场景和物联网等领域都是当前较为热门和重要的应用场景，数据安全在这些领域具有重要的意义。

- **平台产品的通用性：**尽管数据安全平台产品针对不同的应用场景进行了规划，但调研结果显示大部分平台产品适用于多种场景。这表明这些平台产品具有一定的通用性和灵活性，能够满足不同场景下的数据安全需求。这也符合数据安全平台产品的一般设计理念，即提供一套综合性的解决方案，适用于多个行业和应用领域。

- **关注度较高的应用场景：**云计算、工业互联网、车联网、智慧场景和物联网等应用场景在数据安全领域的关注度较高。这些领域在实践中面临着大量的数据交互、数据存储和数据处理，因此数据安全成为重要的关注点。数据安全平台产品厂家将重点关注这些领域，并为其提供相应的数据安全能力，以满足市场需求。

综上所述，调研结果表明，数据安全平台产品针对云计算、工业互联网、车联网、智慧场景和物联网等应用场景具有较高的关注度。同时，大部分数据安全平台产品具有通用性和适用性，能够满足多种场景下的数据安全需求。这反映了数据安全产品厂家对于市场需求的理解和产品设计的灵活性。

（四）制约数据安全平台发展的因素

在当今数字经济规模快速扩大的背景下，组织机构对数据的应用场景和需求都日趋复杂。不断发展的数据安全性、合规性和数据共享需求，要求组织机构的数据安全领导者具备数据安全运营的理念。

这些要求本应是数据安全平台发展的动力和契机，然而，有几个重要因素阻碍着数据安全平台的进一步发展，包括：

- **数据安全建设思路落后。**传统的信息安全观念往往过于强调对数据的保护，在产品功能需求和数据管理流程上施加了多重限制，导致员工无法充分利用数据。而部分数据安全厂商过于专注挖掘其产品的优势功能，而不是将其产品组合重新构建为综合数据安全平台，缺乏对数据安全持续运营模式的远景考虑。为了在数据广泛共享的基础上提高数据的业务价值，无论是作为数据安全产品的用户单位还是数据安全服务商，都需要建立更先进的数据安全管理策略，把数据治理体系和数据安全平台建设相结合。

- **数据安全管理协作困难。**当前的数据安全体系建设存在管理碎片化问题，不同的数据管理团队和系统无法有效协同。为了成功地实施数据安全平台，各个团队，包括业务团队、数据安全团队、合规团队和专家，都需要高度协作。在大型机构如政府或集团企业或者其他大型商业机构中，复杂的组织架构结构、众多的利益相关方和冗长的决策流程和众多的利益相关方往往导致数据安全平台的推广受到阻碍。

- **敏感数据的精准识别与管理。**尽管许多数据安全服务商声称其产品具有数据发现功能，但在实际应用中，这些工具往往不能准确识别真正的敏感数据。例如，对于一个简单的日期数据，系统可能无法区分它是出生日期还是交易日期。而缺乏工具的自动化支持，组织机构就需要投入巨大的资源执行精细化的数据识别和标签，并且效果往往不够显著。为了提高数据安全，平台需要能够精准识别数据的类型和级别，并采取有针对性的适当保护措施，如数据脱敏或加入数据水印。

- **数据安全平台的集成挑战。**当前的数据安全体系中，单独的安全设备和云上产品常常运行在孤立的环境中，这种分散的状态使得它们难以形成一个统一、高效的安全平台。尽管这些设备和产品具有高度的专业性，但它们之间的缺乏协同会导致安全盲区，增加风险。此外，当企业尝试将这些孤立的工具整合到基于云上数据安全平台或数据安全即服务(DSaaS)中时，可能会面临与现有业务流程不兼容的问题，这不仅会影响业务的正常运行，还可能增加额外的成本和复杂性。

（五）数据安全平台发展趋势预测

随着数字经济的崛起，数据安全平台正逐渐成为企业运营的关键支柱之一。社会对数据隐私和安全的需求预期持续上涨，迫使数据安全平台不断更新迭代，以满足不断提升的客户需求，以及更严苛的法规标准。

核心驱动技术，如云计算、大数据、AI 以及特别的区块链技术，为数据安全带来了创新的视角，其特性使得数据安全有了更高的可靠性。这些平台将实现从实时追踪到全方位的自动化响应，同时整合满足法规要求的审计功能。而在技术和能力上，结合了 NLP、机器学习等先进技术，以及多源数据采集等功能，确保了数据的高精确性和安全性。

与此同时，数据安全平台也将加速从孤立的安全产品转变为一个综合的平台，这有助于最大化数据的业务价值。未来，数据安全平台将更注重于一致且可视化的安全策略、语

义功能的数据分类、高度集成的策略控制以及通过 API 和云交付的高级集成，以实现简化部署和更广泛的应用，推动组织的数据安全管理成熟度不断提升。

6.2. 数据安全平台国内外对比分析

（一）市场方面

近年来，数据安全市场规模不断增长。据最新调查数据显示，2022 年数据安全市场规模为 102 亿，同比增长 15%，而数据安全平台类的产品占比在 15%左右。国内市场目前具备数据安全平台类产品的企业超过 50 家，具有一定的市场规模和落地应用，且具备不错的发展前景。根据 Gartner 预测，到 2024 年，30%的企业将应用数据安全平台，未来 2 年内数据安全平台在全球范围内的渗透率有望迅速提升。

从安全厂商的布局来看，全球主流的数据安全头部厂商已经通过收购及合作等方式构建数据安全平台能力，可观察到从 2020 年开始相关并购的数量开始迅速增长。例如，IBM 与 1touch.io 签署了经销商协议，以在 IBM Security Guardium 产品组合中提供发现和分类功能。Imperva 收购了 jSonar 以扩展其数据安全平台的覆盖范围和集成可能性。Informatica 收购了 GreenBay Technologies 获得了数据治理等 AI 能力。Netwrix 收购了 Stealthbits 为其数据安全平台添加 DAG 和 SQL 保护功能。PKware 收购了 Dataguise 为其数据安全平台获得数据发现和脱敏功能。Varonis 收购了 Polyrize 以将其数据安全功能扩展到 SaaS 应用程序。

同样地，在国内市场，一些专注在数据安全领域的龙头厂商，比如天融信、观安信息、美创科技、启明星辰等，也通过对产品线的扩展、整合及优化，已经发展出成熟的数据安全平台，数据安全的平台化也将成为国内数据安全市场的重要趋势。

本次调研数据显示，原有网络安全增加数据安全业务的厂商基于生态优势，开发更多接

口对接不同安全能力组件实现联动联防；而专业数据安全厂商更多的是融合自有安全能力组件，面向多云环境提供复杂数据资产安全管理、数据流动安全管控、数据安全风险监测等能力。此外，数据安全领域的新兴创业公司在数据流转全链路追踪、API 监测与管控、隐私计算等方向也取得了重要突破。各大厂商的数据安全产品能力均呈现快速提升的态势，推动中国数据安全管理平台产品从整体上快速成熟，也让市场竞争更趋激烈。

（二）技术方面

全球数据安全管理市场已经进入快速发展阶段。目前来看，国外企业发展较早，的技术水平和服务经验仍然相对较为成熟，具有较高的安全性和稳定性。

Gartner 把数据安全的相关概念分成了人员流程层、DSP 数据安全平台层、辅助的数据安全基础架构三层，DSP 处于中间。下图从顶层规划的角度，从甲方视角分层定义了数据安全所需的各类能力，区分了数据安全的基础能力。

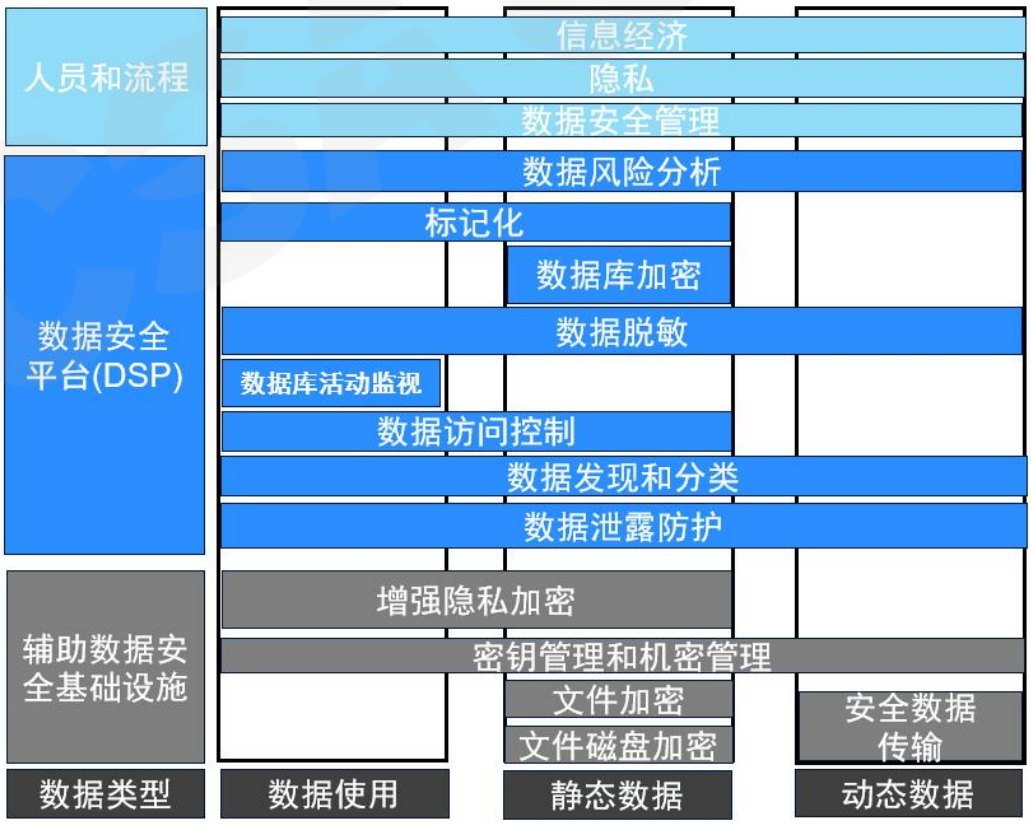


图 5 数据安全平台成为核心主导力量的相关数据安全概念

人员流程层主要通过处理定义的数据策略和流程保护公司数据，并主要通过 DSP 技术执行。辅助的数据安全基础架构包括了基础通用的数据安全能力，如增强隐私加密、密钥和机密管理、文件加密、磁盘加密、安全数据传输。

在国内，众多头部数据安全厂商基于数据安全平台，已构建出全方位覆盖数据安全使用和流通的一体化解决方案。

图 6 一站式数据安全治理运营平台

国内的数据安全治理运营平台致力于提供完备的解决方案，采用数据分类、分级管控和数据流转监测为核心，目标是实现长期有效的数据安全管理。目前，国内优秀的数据安全平台可涵盖数据分类、备份、恢复、加密、安全策略下发、风险可视化等关键功能，并辅以安全审计及日志分析工具。它们为企业提供全面的数据资产梳理，协助企业精确识别数据资产的暴露面和潜在风险。在技术架构上，可支持分布式扩展，拥有出色的水平扩容和易扩展性，同时还内置风险分析的专家经验模型，确保全链路的智能溯源。

在国家对技术创新支持力度不断提升的大背景下，数据安全产业链各环节相关主体将持

续加大在人工智能、区块链、密态计算等基础通用技术方面的研发投入，为数据识别、数字水印、隐私计算等数据安全关键技术的能力提升和创新发展提供有力支撑。应用领域的逐步拓展将推动数据安全技术的持续演进。

6.3. 建设数据安全平台的建议

基于用户对更高级别数据安全的需求，以及产品能力的快速成熟，更多的组织机构会采用数据安全平台进行数据安全建设；另一方面，组织机构也需完善管理体系，包括但不限于完善管理组织、制度流程、技术保障能力和成熟度评价指标等。

对于如何建设成熟的数据安全平台并加以有效管理，以下是几点重要建议：

- **重塑数据安全架构并加强团队合作：**重新审视以数据为中心的安全架构，并组建专业的数据安全团队，加强与组织内的利益相关方合作，明确资源瓶颈并解决潜在问题，共同规划长期的数据安全策略。

- **全面扩展数据安全平台功能：**规划并构建全面的数据安全平台路线图，基于数据流转过程和场景，整合数据处理、标签、加密和脱敏等功能，并与安全供应商充分合作，降低实施复杂性和成本。

- **集成化与技术创新：**注重数据安全平台的技术集成，如 API、云服务等，将各种功能融合在一起。同时，依据行业标准和合规要求，不断推进数据安全平台的技术创新和完善。

- **策略更新与持续优化：**定期更新数据安全策略，确保与最新的行业标准和技术趋势一致。通过持续的管理和运营，确保数据安全的高效、完备和标准化。

由于数据安全治理工作本身的复杂性和多样性，不是单一产品或平台就能解决的问题，

需要组织机构的管理者从运营管理的角度付诸长期的努力。目前，要以数据安全平台为中心实现数据安全运营，还缺乏成熟的解决方案。如果数据安全平台能够提供“运营管理”模块，将人员、组织、安全策略全部涵盖，结合管理能力和技术能力，将为政企机构的数据安全治理及运营提供支撑，从而推动实现高质量、标准化的数据安全运营。

7.数据安全平台的实践案例

7.1. 天融信数据安全管理解决方案

7.1.1. 平台简介

（一）能力描述：

天融信数据安全管理解决方案以法律法规为指导依据，以数据安全管理平台为核心，以数据安全治理咨询服务为辅助，综合运用自然语言处理与多层次综合识别分类技术、多引擎纵深化风险分析识别技术、多源异构数据采集等先进技术，帮助用户实现数据资产全面管理、数据资产分类分级、数据访问权限管理、生命周期风险监测、告警流程闭环处置、多维态势综合呈现，最终实现数据全生命周期的可信、可管、可控、可追溯。

图 7 技术架构

（二）功能概述：

天融信数据安全管理平台总体架构分为防护组件、采集分析、管控应用、态势呈现共 4 层。防护探针层，由数据防泄漏、数据库防火墙、数据脱敏等数据安全防护设备组成，为数据安全管理平台提供能力支撑。

采集分析层，将防护组件中获取到的企业数据安全相关数据采集至数据安全管理平台中，经过清洗与标准化后，进行数据生命周期安全分析和专题场景分析，发现网络中存在的数据安全风险。

管控应用层，提供数据资产管理、数据分类分级、数据安全防护、告警与响应和数据安全审计共 5 大管控应用，满足数据安全管理需求。

态势呈现层，从数据资产分布、数据安全流转、数据安全告警、数据安全风险、数据资产防护等角度对网络中数据安全状况进行可视化呈现，帮助安全运营人员，直观掌握数据安全发展态势。

- **数据资产自动发现**

可根据预定任务自动进行数据资产扫描，并基于行业分类分级标准形成敏感数据特征库，从而减轻人工识别工作量，实现敏感数据识别自动化。

- **全生命周期态势评估**

从采集、存储、传输、使用、共享、销毁等数据全生命周期维度对数据安全风险进行监测告警，从数据资产分类、数据流转过程、敏感数据分布等多维度对告警信息进行态势评估，直观展示风险以及潜在的威胁，为安全策略管理提供依据。

- 分析建模零代码搭建

内置关联分析引擎，融合大数据分布式计算等技术，通过可视化拖拽算子算法实现零代码关联分析模型搭建，提高分析模型搭建效率，降低模型搭建技术门槛。

- 防护组件快速扩展

采用多种方式与防护组件进行对接，通过可视化配置快速接入第三方数据安全设备以进行安全数据采集，并基于特征匹配、字段提取等灵活扩展技术应对不同厂商、不同型号安全设备的扩展需求。

- 全流程数据安全运营

提供数据资产管理、数据安全威胁分析监控、数据安全告警跟踪处置、数据安全策略管控等功能，全面支撑数据安全运营工作。

7.1.2.实践案例：某海关单位 2021 年数据安全管理平台优化完善服务采购项目

（一）项目背景

本项目以海关数据为核心，采用两级部署架构，覆盖总署及 13 个重要二级关口，进行数据安全管理平台建设，制定海关行业数据分类分级标准，制定海关特色数据防护体系与数据安全风险监测预警机制，实现海关数据安全统一管理。

（二）建设内容

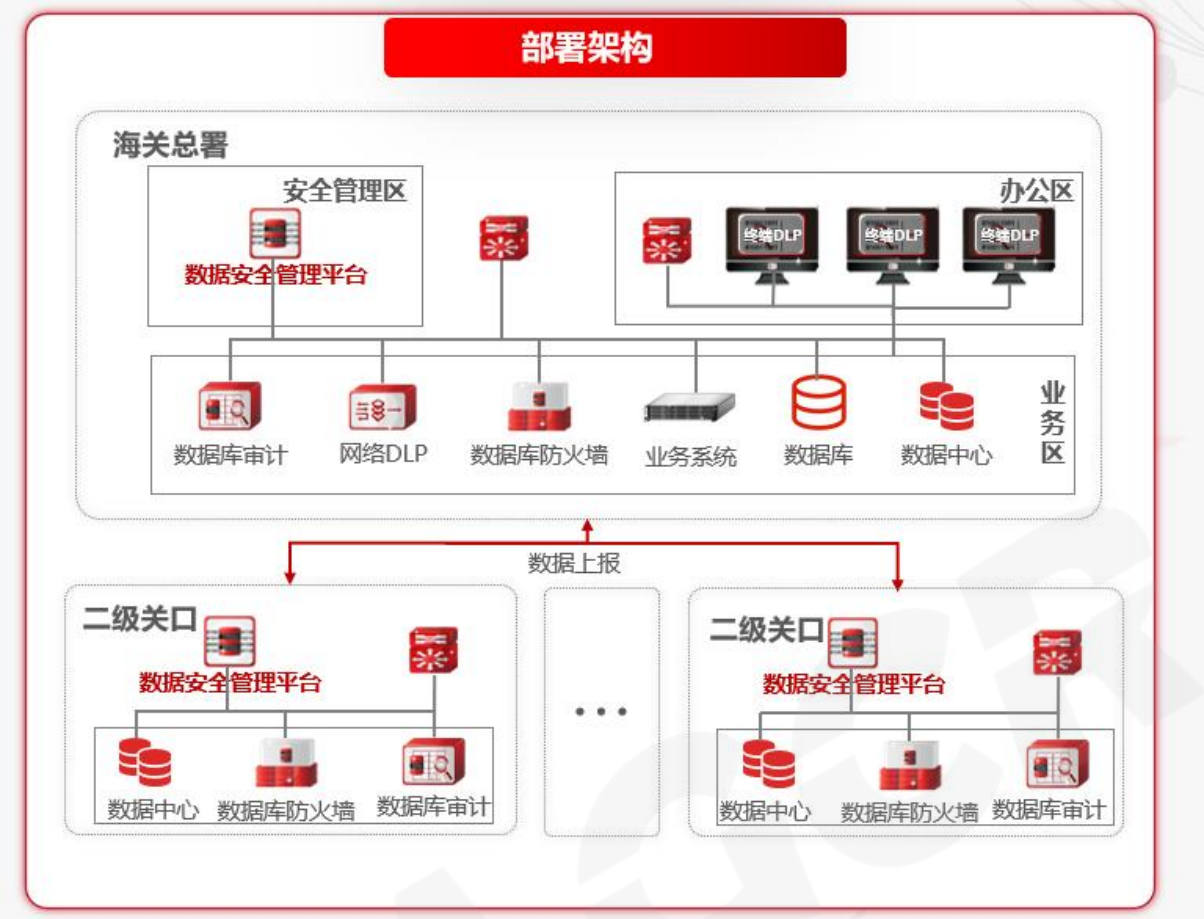


图 8 部署架构

某海关单位为响应《网络安全法》《数据安全法》关于个人信息保护及重要数据保护的要求，落实《海关数据安全分级管理办法》《海关业务数据管理办法》要求，在海关三中心以及十三个关口建立了数据安全管理平台、治理平台，实现了数据资产梳理、安全数据治理、数据安全风险分析等能力，提升了数据安全管控能力。

大数据治理平台：实现海量数据采集、存储、转发、检索功能，建立安全数据传输接口标准规范、日志采集接口规范。

数据安全管控平台：实现数据资产的扫描发现、入网管理、分级分类、UEBA、资产异常告警、数据流向分析、全国数据安全态势大屏等能力。

平台基于对资产探测和数据分类分级扫描，结合人工录入补充，收集的全面数据，针对所关注的数据资产分布情况，从字段级、文件级、数据库等资产角度，进行级别、类别分布分析，分类分级关联关系分析，并以饼图、条形图、关系图等可视化图表形式进行可视化呈现。

通过各类数据安全防护探针采集数据安全风险数据，并经过平台进行深入整合分析，生成高准确度的数据安全风险告警信息，并从账号、资产、应用、风险等级、发展趋势等角度进行告警分析与可视化呈现， 全面掌握数据安全告警情况。

通过各类数据安全防护探针采集数据安全风险数据，并经过平台进行深入整合分析，生成高准确度的数据安全风险告警信息，并从风险级别、生命周期阶段、发展趋势等角度进行告警分析与可视化呈现，把握数据安全风险重点及发展态势。

项目分期建设、逐步深化。一期：总署数据安全试点初探；二期：13 个二级关口推广应用；三期：总署深化应用。两级部署、统一管理：通过总署－二级关口两级架构，将二级关口数据安全情况上报至总署，实现海关数据安全统一管理。全面建设数据核心：以海关数据为核心，围绕数据安全生命周期，通过数审、DLP、数据库防火墙、数据安全管理平台，实现数据资产梳理、分类分级、安全防护与监测预警等多角度进行数据安全管理。

（三）建设成效

天融信数据安全管理解决方案已实际应用在某海关 2021 年数据安全管理平台优化完善服务采购项目中。通过本项目完成了海关数据安全管理体系设计，利用数据安全管理平台及数据安全防护组件为技术抓手，覆盖全国海关，共部署平台 47 套、探针 140 套，对全国海关信息中心、数据中心广东分中心以及 13 个二级关口的数据资产进行治理改造，减少人员投入约 60%，大幅提高数据安全管理工作效率。

7.2. 观安观智数据安全管控平台

7.2.1. 平台简介

（一）能力描述

观安观智数据安全管控平台是一款以数据为中心，以业务安全为目标的一站式解决方案，旨在赋能企业数据安全治理。平台能力框架满足 IPDRR，覆盖数据全生命周期安全管控，实现数据安全风险事前识别、事中预警、事后处置，提供常态化、一站式运营工作支撑，平台提供四大核心能力：

- **【盘清家底】梳理数据资产、绘制数据地图能力。**

通过主动扫描和被动探测技术，发现企业内的数据源，并使用自动化分类分级引擎对数据进行编目，形成企业数据资产清单、分类分级清单等。创新性地使用数据荧光测绘引擎对数据流向进行绘制，形成数据流转地图。帮助用户了解有哪些数据，分布在哪，流向何处，为明确保护对象，洞察数据风险提供有力基础。

- **【风险监测】洞察数据全生命周期风险能力。**

以数据全生命周期为依据，全面识别数据合规风险（如超期超限存储、未脱敏、未加密等）、API 风险（API 脆弱性、明文密码使用等）、用数行为风险（如过频过量、访问绕行、蚂蚁搬家等）、异常流动风险（如未知流向、未备案流动、超合约流动等），利用基于主体的风险降噪算法，提高预警有效性。帮助用户洞察企业潜在的数据安全隐患，感知数据安全态势。

- **【联防联控】自动化的联防联控能力。**

针对识别的数据安全风险，依据安全责任体系，通过建立安全体系一致化分类分级标签，自动化构建响应和处置机制。可以联动脱敏、水印、加密、网关等系统，形成数据安全联防联控体系，增强快速响应能力，提高运营价值。

- **【审计溯源】智能的审计溯源分析能力。**

全面审计监控范围内的敏感数据流动，提供多维度画像分析功能，全面分析有哪些渠道访问目标数据，有哪些人访问过特征渠道以及目标泄露人员的数据访问路径，从而快速定位泄露源头，降低再次泄露的风险。

此外，依托全生命周期度量体系，可以量化企业数据安全能力成熟度，帮助企业发现能力薄弱点以加强建设。观安观智数据安全管控平台已经成功应用于运营商、能源、政府、金融等多个行业，用于帮助企业实现自身的数据安全治理、数管安全能力管控、多组织间的数据安全监测监管等多种场景。为组织提供数据安全大脑能力，全方面推进数据安全运营工作。

（二）技术架构

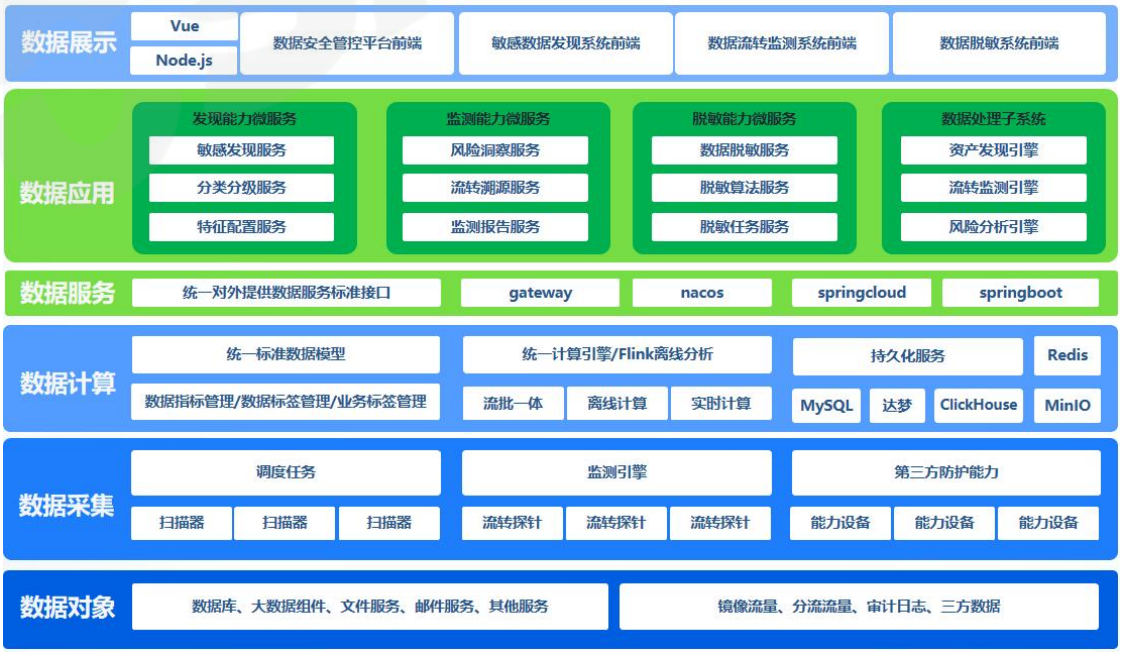


图 9 技术架构

（三）功能概述

- **资产梳理：**通过资产梳理，理清各资产、API、账号、IP 的业务属性以及数据流转概况，从“乱成一锅粥”变成“一本清晰台账”。

- **分类分级建设：**数据发现、数据识别、数据分类、数据分级等核心功能帮助企业实现数据的分类分级。

- **数据资产清单：**数据经过业务分类和安全分级后，形成数据资产清单。

- **API 接口梳理：**通过接口梳理，持续发现所有 API，包括影子 API 和僵尸 API，通过分类理清各 API 的业务属性以及数据流转概况。

- **账号提取：**通过账号提取，涉密人员发现，识别自然人，定位追踪到具体责任人。

- **流转测绘：**基于全链路的数据安全治理结果动态呈现。从数据标识及分类分级到数据存储位置、调用接口、流转链路和访问人员进行动态展示。基于全链路、多层关联的审计要素，贯穿人、数两个维度的双向溯源（以人追数、以数追人）机制，实现高效、准确的事件定位定责。

- **风险监测：**多级管线处理技术，对原始数据访问记录分级处理，识别资产、敏感发现、业务/扩展特别识别、流转行为识别、风险指标预计算、风险策略引擎，可以逐级富集信息，充分挖掘分析数据访问行为，提高流转行为分析和风险精准度。

- **生命周期标识：**对完成分类分级任务和核查任务后形成的完整数据资产清单，通过设置任务的形式，根据部门、业务系统、是否已生命周期标识等筛选条件筛选出一批聚集的数据资产形成一个任务，从任务的维度对其完成生命周期进行标识。

- **脱敏服务：**确保数据脱敏工作标准化与规范化的同时，简化了对其操作的复杂性，

实现了数据脱敏“过程可重复、结果可验证”。

- **审计溯源：**可对访问行为进行线索回溯、流转地图和统一检索等多维度溯源能力，定位泄漏源头。

- **预警处置：**风险预警发生后，用户可通过不同的处置方式对风险进行处置，包括加白、忽略、仅告警不通知、线下处理等方式，系统自动对处置后的风险进行实时监测，发现风险完成处置后自动归档。若风险在处置后仍未完成，则系统会再次进行预警，告知用户进行二次处理。

- **开放对接：**各原子级能力的集合，其他包括敏感识别、分类分级、脱敏、水印、数审、溯源、合规检查等。通过策略中心按需组合配置和编排多种管控原则，实现可编排的安全管控策略，通过下发的管控策略进行多种防护能力的联动，可视化监测多种防护功能的实施完成情况。

- **基座支撑能力：**对外提供接入各种开放式的原子级的处置能力和安全防护能力，以及对外数据、策略和日志的互联互通。

7.2.2. 实践案例：某运营商集团数据安全管控平台

（一）项目背景

该平台针对某运营商是典型的集团加各省分公司及专业公司的组织结构。其中业支和网络部是主要是信息化部门，都有安全需求。各省公司也会对应的业务网络部对应，集团侧起到专业指导和检查作用；安管中心《xx 客户信息安全保护管理规定》企业管理办法合规诉求。

业务上：缺少对整个 IT 领域数据的统一策略防护和有效管控，需要信息化系统满足业

务安全合规需求需要支撑 10 省中心两部委考核、属地管局考核；技术上：多地资源池，多网域情况下的统一管控的技术需求，低运维成本，由于网络限制，每条网络链路都需要显式开通，尽量减少网络策略的复杂度 。

（二）建设内容

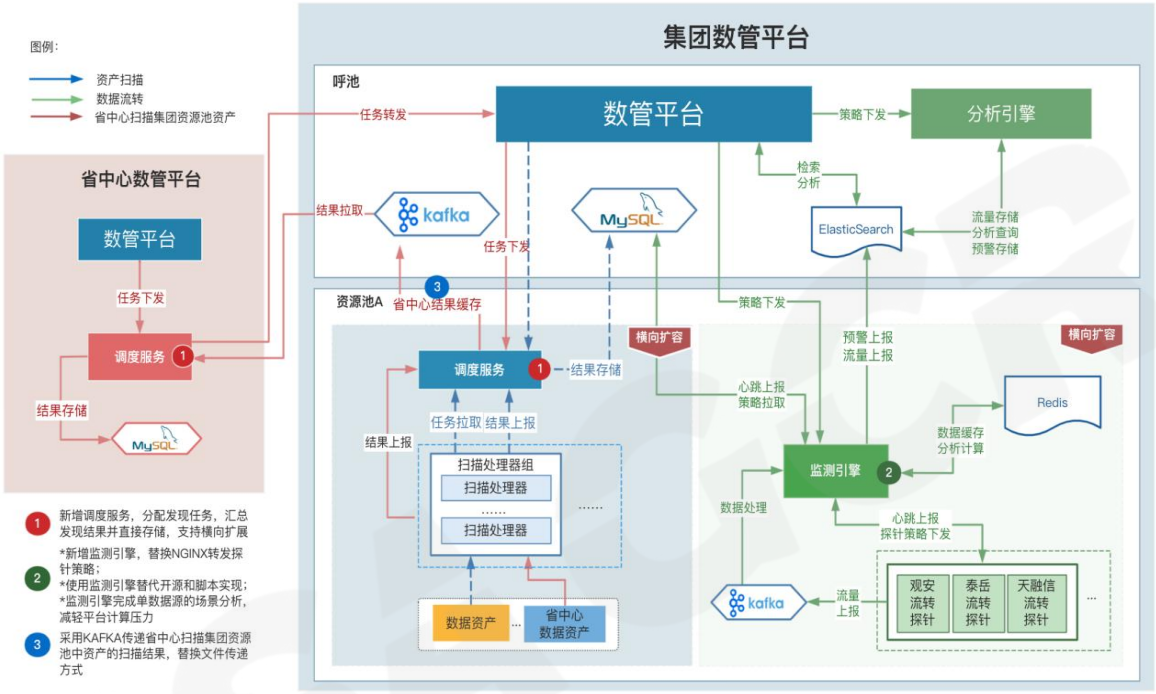


图 10 建设内容

- 数管平台覆盖公司各业务部门，实现对数据发现、集中化策略管理、数据泄露分析、数据安全运营等能力。

- 实现基于流量的生产运行和生产运维数据安全防护实时监测能力，并完成数据扫描器的数据发现识别能力优化和推广工作。

- 完成各业务部门的脱敏策略效果验证，数据安全事件实时监控和处置；并实现多中心数据安全纳管。

（三）建设成效

- 实现企业敏感数据的自动化识别与分类分级管理，敏感数据传输的安全监测。满足合规要求、监管要求，满足基础性数据安全、数据全生命周期安全、技术能力建设等数据安全考核要求和评分标准。

- 实现企业敏感数据存储的安全监测，保证敏感数据存储符合管理要求。监控数据暴露和数据流动情况，对过频过量的异常访问行为进行监测，以免引起数据安全泄露的风险。对内部人员的业务操作行为进行监控，避免个人敏感数据的恶意访问和跨权限的账号滥用等风险。防止内部员工违规操作，窃取个人敏感数据，贩卖获利。

- 管控了 500 个业务系统，10000 项数据资产，150 万张表，5 亿个字段和 1 万个对外接口；有力支撑了常态化迎检。降低数据在采数、传数、用数和数据要素流通等场景下的风险，促进数据安全流动和有序高效利用。做好数据防泄漏、数据防破坏和数据安全合规的工作，做到对合规变化和风险变化能及时应对，使数据可以安全地对外服务和赋能。

- 满足企业内部考核的数据安全管理、运营、技术的整体闭环管控要求和风险评估标准。防止对分级管控的系统和数据，进行超期超限访问。尽量做到领域内的各项数据处理和访问合规。以及满足部门做数据安全规划时，对数据使用业务的管理要求。

7.3. 启明星辰数据安全治理管控平台 DSMP

7.3.1.平台简介

（一）能力描述

启明星辰数据安全治理管控平台（DSMP）以数据为中心，融合零信任理念，基于场景化的思路进行设计，在对数据资产自动发现、分级分类的基础上，根据不同场景的安全

需求和安全风险，统一制定安全策略并调配底层能力组件，实现数据全生命周期管理。数据安全治理管控平台（DSMP）同时提供对安全运营服务的支撑，使得制度、规范、流程、风险评估、安全能力、安全策略形成闭环，从而为数据安全构建起一套综合的防护体系。

（二）技术架构

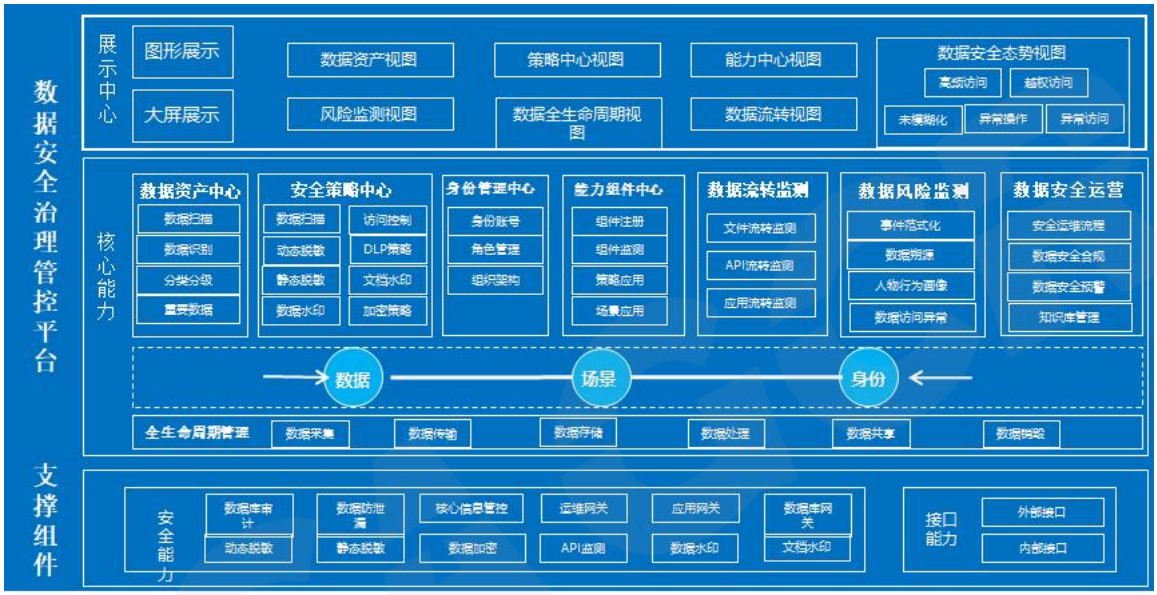


图 11 DSMP 数据安全治理平台设计架构图

（三）功能概述

数据安全治理管控平台（DSMP）的核心思路是，面向不同类型、级别的数据，基于场景，进行统一的安全策略管控。

- **识别数据，对数据进行分类分级**

通过自动化手段发现各类数据资产，包括并不限于数据库、大数据、文件等。

根据用户行业的分类分级规范，自动化对数据进行分类分级，并可以进行人工复核操作。

- **数据安全策略统一管理制定**

通过丰富的自定义安全策略实现数据的安全管控，包括并不限于敏感数据发现、访问控制、加密、脱敏等策略。

对数据安全策略能够集中控制、展示和管理，对数据安全的行为、防护能力集中控制管理，支持策略创建、增加、删除、修改等操作。

数据安全策略管理中心提供数据安全防护能力输出和数据安全防护策略的任务下发。

- **识别不同数据场景应用策略**

数据采集场景：通过系统录入、数据接口服务器、数据库交互、文件导入等进行采集。

数据传输场景：通过应用互传、FTP 服务器、终端互传、终端外发等方式实现业务的设计和开发时进行落地。

数据存储场景：数据存储包括主机存储、数据库存储、终端存储。

数据使用场景：包括系统运维、业务开发、开发测试、外部用户访问应用场景。

数据共享场景：包括库表共享场景、文件共享场景、API 接口场景。

数据销毁场景：包括数据库数据删除、服务器数据删除、终端数据删除。

- **通过调度安全组件，实现数据安全的有效管控**

实现对数据安全能力组件的上报信息的采集，以及对各能力组件的接口配置，方便在上层进行事件存储、分析、策略管理等。

数据安全的安全防护能力包括：统一身份认证、应用安全网关、运维安全网关、数据静

态脱敏系统、数据动态脱敏系统、页面水印、文档水印、数据水印、数据库审计、数据库访问网关、数据防泄漏等安全能力组件。

- **数据安全风险态势的集中展示跟踪**

提供包含数据资产视图、策略中心视图、能力中心视图、风险监测视图、数据全生命周期视图、数据安全态势视图等多种丰富的可视化展示。

7.3.2.实践案例：某城市数据安全一体化运营中心建设

（一）项目背景

某城市大数据管理局成立至今，随着某城市新型智慧城市建设推进，基于数据共享和流程变革的智慧城市管理服务不断投入运营，极大地提升了社会管理服务运行效率，但数据在整合共享过程中也面临众多安全风险：

- 数据从四面八方汇总在一起，其中不乏大量敏感数据，集中的数据更容易成为攻击的目标；
- 缺乏对内部人员业务访问权限的精细化管控，难免出现违规查询、导出，甚至是修改数据行为，给数据泄漏造成极大隐患；
- 政务数据在各政府部门之间流动、共享和交换，数据存在于数据域、业务域、交换域、终端域，数据交换各环节如果不协调一致，极易造成数据泄露。

（二）建设内容：

针对以上情况，启明星辰专业技术团队进行了如下的建设方案。

1）数据安全治理建设咨询

- **管理组织建设**

建立数据安全管理的组织架构，明确数据安全管理人员职责权限及各个环节运行沟通协作机制。

- **标准规范建设**

建立健全覆盖数据全生命周期的安全管理制度规范，使数据安全管理组织管理有规范可循，有流程可依。

2）数据安全管控平台（DSMP）建设

- **管理平台建设**

建设覆盖数据安全管理全链条的数据安全管理平台，对数据安全操作行为进行有效管控，对数据安全信息进行研判、预警、展示和处置。

- **技术体系建设**

规划大数据中心所有安全域，采用数据加解密系统、数据防泄露、数据堡垒等多种技术和工具，全面建立大数据中心安全技术体系。

建设成果如下图所示：

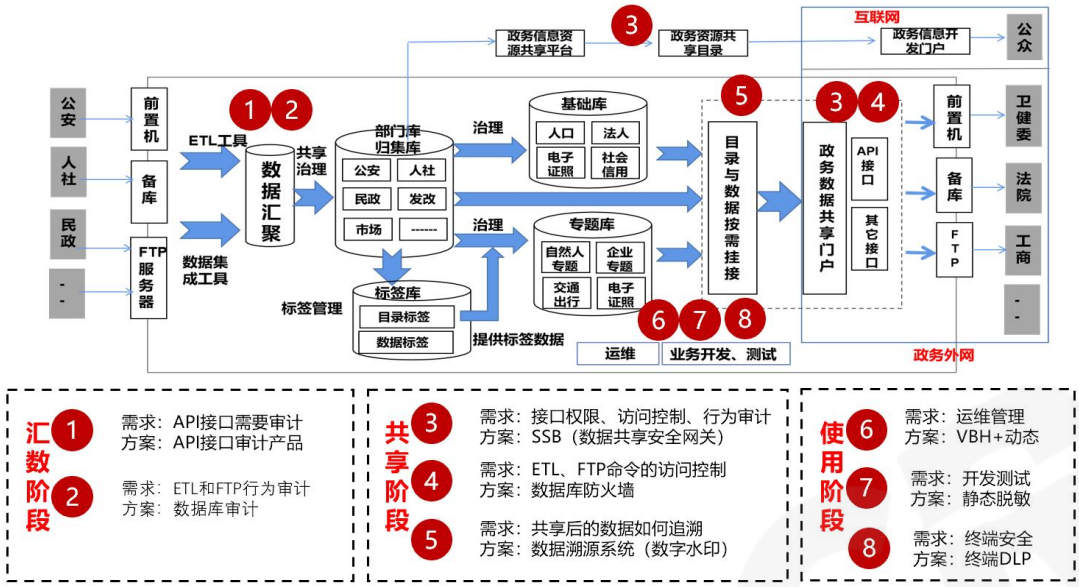


图 12 建设成果

- 建立数据安全管理、运营体系
- 运营体系建设

建立专业的数据安全运营队伍，对数据安全进行管控、评估和咨询，确保城市大数据中心安全体系可靠运行。

（三）建设成效

- 管控某市共享交换平台 20 余个数据库；部署了数据安全管理平台、数据库脱敏、API 管控探针、数据库审计、堡垒机等 20 余台设备；
- 编制了某市公共数据分类分级指南、数字相关数据安全标准等 3 份标准，优化数据安全管理办法及规范文档 40 余份，形成了涵盖近 40 个资源库、1777 张表、61656 个字段的分类分级清单，制定了字段识别策略共 8281 条、一级分类 410 个 、二级

分类 196 个、三级分类 127 个、 四级分类 9 个，全面监控 1600 余个 API 接口的安全风险。

- 实现数据安全三个 100%：敏感数据识别率 100%、数据资源分类分级 100%、敏感数据安全传输 100%。
- 建立了数据安全管理和运营体系，管理无死角，技术防得住。
- 首个政务数据中心通过数据安全能力成熟度（DSMM）三级认证

8. 展望

自《数据安全法》于 2021 年 9 月 1 日开始施行后，我国数据安全领域迅速崛起，其中数据被正式视为核心生产要素，数字经济日新月异地推进着国家的进步，数字中国建设的蓝图已经展开。在提高数据的经济价值时，数据保护的任务也日益加重。

此次调查表明，数据安全技术与产品正在经历革命性的创新与改进。由于众多角色共同发力，如监管机构、数据经营者、安全服务商以及研究机构的齐心协力，我们有理由坚信我国的数据安全产业将趋于完善。

企业数据安全治理首先需要明确数据安全治理目标和策略、建立组织机构，进而进行数据资产识别和分类分级，然后完善数据安全技术体系和工具平台的建设。使用数据时，需要不断优化数据安全的管理策略。通过选择高水平集成能力的数据安全平台产品，根据实际需要共享数据和流转数据，从而实现数据的最大化利用价值，达到数据保护和利用的平衡。数据安全的核心是支撑组织机构的业务使命，并最终通过数据安全运营使这种能力常态化体系化。

作为前沿技术的倡导者，云安全联盟大中华区将继续推动数据安全技术的发展。鉴于本研究报告是我们在数据安全领域的首次尝试，难免存在不足之处，我们的研究团队将在今后会持续优化改进，进一步完善。同样，我们欢迎广大读者给予反馈，我们可以更好地提升我们的工作。

鸣谢

感谢云安全联盟大中华区成员单位天融信和观安信息对本报告的赞助支持，但不影响云安全联盟大中华区对本报告的编辑权和所有权。

天融信科技集团 创始于 1995 年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。天融信作为国内网络安全领域的先导者，始终关注技术与实际应用场景的结合，面向政策合规、行业监管、安全运营、工业数据安全等多样化数据安全应用场景，天融信数据安全管理平台可帮助用户构建数据安全感知中心、决策中心和指挥中心，现已在运营商、海关、能源等多个行业领域及国家工业互联网数据安全课题中成功应用。

观安信息 是一家提供大数据+泛安全产品与服务的高新技术企业。公司聚焦数据安全、网络空间安全、5G 安全、人工智能安全、工业互联网安全及公共安全等核心方向，为运营商、政府、金融、电力、公安、医疗等行业用户提供全面的信息安全解决方案。公司采用多城市多总部模式，设立多个实验室，业务覆盖全国。是联合国训练研究所上海国际培训中心大数据应用与安全培训基地、联合国工业发展组织上海国际智能制造促进中心专家组成员；是国家重大活动网络安全保卫技术支持单位、工信部专精特新“小巨人”企业、5G 创新企业、上海市高新技术企业。核心团队有着 20 多年信息安全专业技术、10 多年大数据分析经验。在国内外竞赛中，多次斩获金奖，多次参与国家重大活动信息安全保障工作。具备网络安全与大数据领域相关的产品研发、集成和专业服务资质。

反馈与报告预告

报告意见反馈

云安全联盟大中华区致力于提供高质量的研究报告，如果您有任何关于本报告的反馈或建议，请通过以下邮箱与我们联系

邮箱：research@c-csa.cn

2024 年报告预告

云安全联盟大中华区计划于 2024 年发布针对云原生安全和 AI 安全领域的神兽方阵报告，我们诚邀行业专家和企业单位积极参与。

参与方式

意向参选的企业及意向参与报告编写的专家可扫描二维码提交您的报名信息：

国际云安全联盟大中华区
电话:0755-86548359
官网:https://c-csa.cn
邮箱:info@c-csa.cn

CSA公众号　　CSA微信号