

数据安全分类分级 调研报告

(2026 年 10 月)

数据安全 分类分级调研报告

数据安全分类分级 调研报告

(2026 年 10 月)

报告信息

报告方向：数据安全领域调研

报告名称：数据安全分类分级调研报告

报告编号：DWC_20261001

主笔分析师：靳慧超 · 数世咨询-战略分析师

分析团队：数世咨询 · 数字安全研究院

报告审核：李少鹏 · 数世咨询-首席分析师

第1章 关键发现

基于数世咨询对数据安全领域的深入研究并结合本次实际调研数据，针对我国数据安全分类分级有如下关键发现：

- ✓ 我国数据安全的建设目标正从保护数据不被非授权使用，逐步走向在保障安全的前提下管理、使用和流通数据，而数据安全分类分级则是实现这一目标的基础。
- ✓ 数据安全分类分级是一种体系化能力，不仅需要实现数据的识别、理解、分类分级，更需要具备以数据流通需求为根本的分类分级安全控制，目前由数据安全分类分级产品和数据安全管理平台共同构成。
- ✓ 企业的数据管理成熟度以及跨部门沟通效率是数据安全分类分级项目顺利落地的最大变量。
- ✓ 数据安全分类分级产品对大模型有 3 种应用方式：第一种以大模型为核心，分类分级全流程由大模型直接处理；第二种以大模型为数据理解核心，主要生成分类分级规则；第三种以大模型为辅助，主要替代人工补充判定工作。
- ✓ 数据安全分类分级产品与服务 2025 年市场规模约占数据安全领域（68.91 亿元）收入 3.6%，目前虽然规模与重要性不成正比但市场需求和厂商预期均呈现出高速增长的趋势。
- ✓ 数据安全分类分级将沿着“智能识别、风险研判、动态治理”持续演进，从大模型驱动的内容理解，到智能化安全影响分析，再到数据汇聚与流通风险分析，逐步实现从合规保障向精细化安全管理，并最终支撑数据安全流通与价值释放。

第2章 代表性供应商

参与本次调研的厂商共有 21 家，均拥有自主研发的数据安全分类分级产品与提供相应服务的能力，且拥有自身优势行业，是该领域的代表性供应商。

注：数据安全分类分级体系和能力由数据安全分类分级产品和数据安全管理平台构成，本次调研以数据安全分类分级产品为主，数据安全平台的调研将在后续工作中开展。



企业在选择数据安全分类分级产品与服务供应商时，可以从“安全咨询专业度、行业认知深度、解决方案与业务场景适配度”进行对比。如希望建设完整的

数据安全分类分级体系，建议选择拥有自研数据安全平台的供应商。

本次报告已调研了绝大部分主流、核心供应商，但由于分析师与厂商的时间、精力等因素，并没有达到 100% 的覆盖度。数世咨询会持续完善各领域内容，欢迎厂商、从业者、爱好者随时沟通。

第3章 定义与概念

数据分类分级最初是一种实现差异化保护的信息安全控制手段，在我国网络空间法治的发展下，主要由网络安全法、数据安全法、个人信息保护法的推动逐渐上升为国家数据安全基本制度。

在网络安全法颁布之前，数据分类分级本身是一种数据管理手段，数据安全分类分级是其在安全场景中的应用，目的是为了实现对不同敏感程度、安全风险的数据采取差异化的保护措施，其建立在企业自身对整体信息系统安全风险的高等级控制能力之上，是早期数据安全的一项最佳实践。

网络安全法实施后，对于数据的保护正式进入了国家网络空间安全法律体系。网络安全法第二十一条规定，国家实行网络安全等级保护制度，并要求网络运营者履行相应义务，其中包括采取数据分类、重要数据备份和加密等措施保护数据。但此时的数据安全仍然是嵌入在网络安全体系之中的，法律制度的基本逻辑是网络需要保护，所以网络中的重要数据也需要保护，数据分类是一种必要保护措施。

2021 年，数据安全法明确指出国家建立数据分类分级保护制度，并进一步明确根据数据的重要程度以及发生安全事件后的危害程度，对数据实行分类分级保护，这也成为了我国数据安全发展过程中最重要的制度分水岭。这意味着法律制度的基本逻辑已经完成了转变，从最佳实践到必要保护措施到基本制度，表明了数据分类分级已经成为决定数据应该获得何种安全保护的核心依据。

注：现在规章和标准层面仍然存在数据安全分类分级和数据分类分级两种表述，但可以认为其两者等同。因为在现行制度语境下，数据分类分级就是以安全保护为核心目标的分类分级，强调安全只是为了突出应用目标（这也是本报告采用数据安全分类分级的目的）。但有一点必须加以说明，即数据分类本身是数据管理的一种经典方法，其自身仍具备极高的独立价值。

这 3 个阶段实际上对应了数据安全保护对象的不断明晰化。第一阶段数据作为信息系统的附属，在保护系统时顺带保护数据；第二阶段数据作为网络中的重

要组成部分，需要进行单独保护；第三阶段数据作为独立的安全治理对象，形成了自身特有的制度体系。

综上所述，数世咨询对数据安全分类分级做如下定义：

数据安全分类分级是，以数据安全治理为目标，以数据识别、理解和安全影响分析为基础，对数据进行分类与分级，并提供数据分类分级结果与安全保护要求之间的标准化映射，为数据实施与其安全风险相匹配的差异化保护提供依据的一种方法。

注：数据安全分类分级是一种方法，而数据安全分类分级产品是一种工具。方法可以广泛存在于整体数据安全能力中，而工具则只负责执行某一项具体的任务。

这里需要明确的一点是，目前的数据安全分类分级能力存在于数据安全分类分级产品和数据安全平台上。数据安全分类分级产品的核心功能为数据识别、数据理解、分类分级，未来将逐步完善安全分析能力。安全分析和安全要求映射能力在数据安全平台上体现，未来将持续加强智能化程度。

数据安全分类分级产品主要关注数据本身是什么、重要程度如何以及确定分类分级结果，主要处理对象是数据资产及其静态存储内容。而数据安全平台进一步关注数据被谁使用、如何使用、向哪里流转以及实际使用过程中是否产生安全风险。

数据安全分类分级是数据安全治理的基础能力，需要结合多种技术和管理才能组成完整的体系，支撑数据安全风险监测与运营。

数世咨询认为，由于数字化业务的实效性和内部风险控制的要求，未来的安全影响分析能力具备延伸到具体业务系统上的可能性，突破安全与业务的界限。但本报告核心研究现阶段以及短期内可能的发展方向，暂不讨论与业务系统融合的情况。数世咨询将持续关注前沿发展，在合适的时间启动相关研究。

第4章 核心洞察

4.1. 数据安全分类分级决定未来安全能力的上限

未来的数据安全要求数据在流通使用的过程中，其原有的安全属性和控制策略能够随着数据同时流转，并根据最终处理主体和使用场景实施动态、精细化的管控，以有效降低数据滥用、误用、非授权使用和数据汇聚、关联引发的安全风险升高，最终达成数据流通使用的目标。

实现这一目标的前提是对数据做全量化的识别以及细粒度的标识，而这正是数据安全分类分级的核心功能。通过数据安全分类分级，我们可以清晰的了解到一个数据属于哪里、敏感程度如何、安全属性是什么，使其在脱离原有系统边界时依然保有所需的安全属性，让数据自身携带可被识别、传递和执行的安全策略，即安全属性随行。

在此基础上，安全能否真正做到与业务融通，取决于分类分级结果是否具备足够的准确性与精细化程度。因为不论未来安全能力进化到何种程度，其本质终究都是服务于业务发展的，都需要根据数据自身的业务属性适配相适应的安全属性、安全策略和安全控制。

传统网络安全以网络资产为保护对象，资产识别的准确性和精细化程度决定了安全控制的颗粒度。网络安全能力的边界在本质上受网络资产识别与管理能力的制约，而现阶段我国网络资产管理仍表现出较强的粗放性，以至于在人工智能技术高速发展的今天仍然处于一种“巧妇难为无米之炊”的窘境。

同样，未来的数据安全以数据为保护对象，数据安全分类分级的准确性和精细化程度将直接左右安全控制的颗粒度。所以更加准确和细致的分类分级结果才可以使安全控制依据业务的特异性需求实现特性化策略和动态变化，打破安全与业务的隔阂，真正促进数据流通和数据要素价值释放。

4.2. 数据安全分类分级已实现自身价值的三级跳

数据安全分类分级的实践于 2018 年前后在我国出现，当时主要作为外贸企业针对 GDPR 的合规应答。2021 年数据安全法实施，其在理论层面升级成为所有企业的合规性适配。2023 年起，由于我国数据要素战略的稳步推进，数据安全分类分级在合规属性之外又肩负起促进数据有效、高效流通的责任。在这期间，数据安全分类分级扮演着不同的角色，完成了自身的价值跃迁。

在早期的数据安全实践中，数据安全分类分级是安全控制的附属能力，此时还未正式出现数据安全分类分级的明确表述，处于一种“有实无名”的状态。其更多隐含在敏感数据识别、个人信息保护、数据库脱敏和加密等项目之中。采用数据安全分类分级的直接目的，通常不是建立完整的数据分类分级体系，而是识别哪些数据属于敏感数据、哪些数据有特殊安全要求，并据此附加相应的安全控制措施。

随着数据安全法正式建立数据分类分级保护制度，使得数据安全分类分级进一步从企业内部的安全技术实践，上升为国家数据安全治理制度的重要组成部分。企业开展数据分类分级的核心驱动力，也由满足具体安全场景，逐步转向满足系统性的法律合规要求。在这一阶段数据安全的发展中，密码改造、数据资产管理、数据安全平台等产品和解决方案逐渐成熟，我们觉察到无论是数据发现、数据识别，还是安全策略配置和安全能力建设，都需要建立统一的数据安全分类分级体系作为基础。数据安全分类分级也开始从安全产品的附属功能，逐渐发展为连接数据资产管理与数据安全管理的必备能力。

紧接着数据基础制度建设和数据要素市场化配置改革不断推进，此时数据安全分类分级的角色又开始发生新的变化，在基于解决保护重要数据的基础上，还需要回答哪些数据可以流通、在什么条件下流通、经过什么处理后可以流通。数据安全分类分级已经突破传统的合规属性，逐渐成为数据安全流通和开发利用的前提和基础。

从为了安全控制而分类分级，到为了法律合规而分类分级，再到为了数据流

通而分类分级，我国的数据安全分类分级已经完成了自身价值的三级跳。

本次调研数据显示，现阶段有关数据安全分类分级的项目中，数据安全分类分级产品和服务为直接需求的占比为 47.9%，并且这一数字表现出持续且强劲的上升趋势。这说明，越来越多企业不再只是为了完成某一个脱敏、加密或合规项目而开展分类分级，而是开始将其视为一项需要长期建设和运营的数据安全基础能力。

这一变化从侧面反映出我国数据安全建设重点正在发生根本变化，从单纯保护数据本身，逐步走向在保障安全的前提下管理数据、使用数据和流通数据。而对于数据安全分类分级，过去是安全控制的前提、现在是数据治理的基础、未来可能成为数据安全流通的语言。

4.3. 企业只为可信任的结果付费而并不是大模型

2025 年以前，传统数据安全分类分级项目仍高度依赖人工，根据部分典型项目实践经验，人工服务工作量甚至可能超过整体工作量的一半。其根本原因在于，传统分类分级产品主要依赖预先设定的分类分级模板和判定规则，产品本身缺乏对数据内容的自主理解能力。

因此，在产品执行之前，需要人工分析待分类分级数据、设计分类分级模板并配置判定规则。产品功能执行之后，对于无法通过既有规则准确识别的数据，仍需要人工进行补充分类和确认。在数据管理基础较差、业务复杂度较高的场景下，无法直接通过既有规则完成准确判定的数据占比可能显著上升，极端情况下甚至可能成为项目工作的主体。

这一现象的本质是由于传统分类分级产品依然延续网络安全基于规则驱动的逻辑，未能实现依据数据理解与分析的自动分类分级。但这并不意味着规则驱动本身存在问题，而在于数据的语义、业务场景或上下文无法被提前形式化为规则时，系统便无法完成准确判定，只能重新依赖人工分析。

2025 年之后尤其是自 2026 年开始，由于大模型在网络安全领域更加成熟的

应用，新型数据安全分类分级产品已经拥有了对数据理解和分析的能力，并且涵盖结构化与非结构化数据，使其从规则驱动升级为智能分析，真正走上了标准化与自动化的路径，实现了工作效率的极大提升。

大模型对于数据安全分类分级的核心能力提升在于对自然语言的理解与关联推理分析，在标准化程度较高、业务语义相对明确的数据场景中，大模型已经能够承担大量原本需要人工完成的数据理解、规则生成和补充判定工作，其分类分级结果在部分场景中已超过初级实施人员并且接近高级服务人员的水平。

但是，由于数据安全分类分级的结果直接作用于后续安全策略和控制，触及安全责任的范畴，导致了数据安全分类分级的最终结果必须由人工确认。而这个责任的最终归属方为企业自身，导致企业只关注结果并不在意实现的过程。

企业本质上购买的是一个可信任的分类分级结果，并不是大模型能力。数据安全分类分级对于大模型的应用，并不会直接改变企业对结果负责的基本逻辑。大模型改变的是分类分级结果的生产方式，而不是分类分级责任的归属方式。

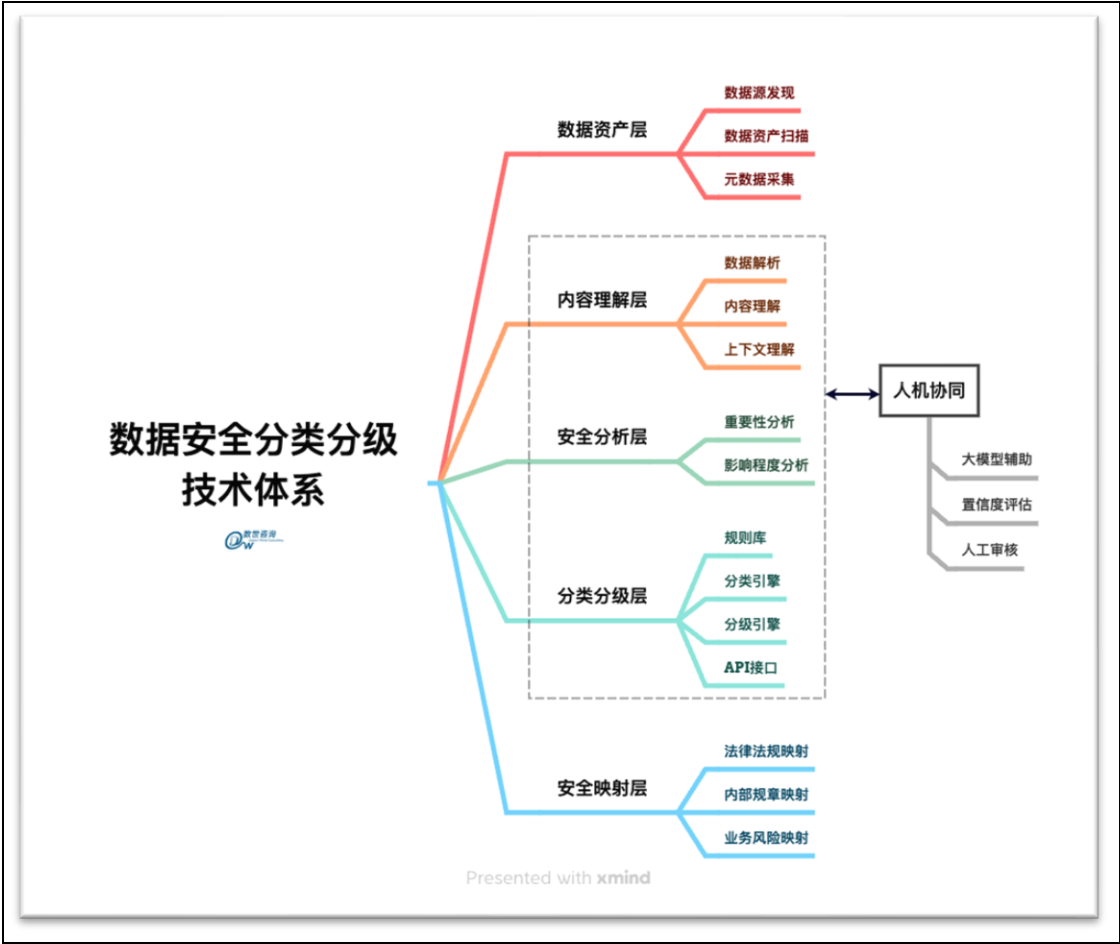
在人工智能安全治理没有形成广泛统一的认知、大模型推理的可解释性没有得到验证的现阶段，大模型最大的价值在于提升了工作效率，大幅降低了人工投入和项目周期。由于算力（企业是否自有、供应商是否提供等）、数据隐私（数据读取权限、分析结果的处置等）等现实问题，企业最终需要根据自身的 IT 环境和风险接受度选择合适的产品。

这也就催生了新型数据安全分类分级产品可对大模型进行不同程度应用的方式。第一种以大模型为核心，分类分级全流程由大模型直接处理；第二种以大模型为数据理解核心，主要生成分类分级规则；第三种是以大模型为辅助，主要替代人工补充判定工作。

第5章 技术体系

根据定义可知，数据安全分类分级技术体系以数据资产识别为基础，以数据内容理解和安全影响分析为核心，通过规则匹配、机器学习、大模型等技术完成数据分类分级，并将结果与法律法规、内部规章及业务风险等要求进行标准化映射，形成与数据安全风险相匹配的差异化安全保护依据。同时通过人机协同机制保障复杂场景下分类分级结果的准确性，实现从数据资产发现、内容理解、安全影响分析、分类分级到安全保护要求映射的完整技术链路。

简单来说，就是识别有什么数据，理解数据是什么，分析发生安全事件后的影响有多大，确定数据属于什么类别和等级，解决数据应该对应什么安全保护要求。最终形成标准化的分类分级结果，并通过接口等方式向数据安全治理及其他安全能力提供结果支撑。



五层之间不是简单的功能堆叠，而是存在明确的前后依赖关系。数据资产识别是基础，内容理解是核心前置能力，安全分析是分级的的重要依据，分类分级是核心判定环节，安全映射则将判定结果转化为可执行的保护依据。

整个体系形成数据源-数据资产识别-内容理解-安全分析、分类分级、安全要求映射-分类分级结果-差异化保护依据的完整数据处理链路。

5.1. 数据资产层

数据资产层主要解决数据在哪里（数据源发现）、有哪些数据资产（数据资产扫描）以及这些数据资产具有什么基础属性（元数据采集）的问题，是分类分级工作的数据基础。

1.数据源发现

数据源发现用于识别组织内部的数据存储和数据资源入口，建立分类分级对象的基础范围。核心作用是确定分类分级工作的数据范围和数据来源。

技术上可通过数据源连接、资产探测、配置发现等方式，识别数据库、数据仓库、数据湖、文件存储等不同类型的数据源，并获取数据源的基本信息。

2.数据资产扫描

进一步扫描数据源内部的数据资产，识别数据库、Schema、表、字段、文件、数据集等具体对象。

通过数据结构扫描、对象遍历、字段发现等技术，可以形

成数据资产清单，建立数据资产之间的基本组织关系。这为后续内容理解和分类分级提供具体对象。

3.元数据采集

元数据采集用于获取与数据理解和分类分级相关的结构、属性和业务语义信

息。核心价值是为后续数据内容理解和分类分级提供结构化、语义化的辅助信息，提高分类分级结果的准确性和可解释性。

注：目前有些数据安全分类分级产品并不采集元数据，但数世咨询认为采集元数据对分类分级的准确性和细粒度起到决定性作用，是必须具备的能力。

采集内容通常涵盖表名、字段名，数据类型、字段注释，主外键关系，长度等结构信息，所属系统、业务域等业务属性，以及其他有助于理解数据含义的元数据信息。

5.2. 内容理解层

内容理解层主要包括数据解析、内容理解和上下文理解，在这个阶段明晰数据具体是什么。

1. 数据解析

数据解析负责将不同类型、不同格式的数据转换为可识别、可分析的内容，将原始数据转换为后续识别和理解可以处理的数据内容。

针对数据库、结构化数据、半结构化数据以及文件等不同数据形态，可以采用相应的数据解析和抽取技术，获取字段内容、数据样本及其结构关系。

2. 内容理解

内容理解主要用于判断数据的实际语义，并不是简单的字符串匹配，而是明确数据代表什么。特别是在字段命名不规范、数据内容复杂或者非结构化数据场景下，内容理解能力对分类分级准确性具有决定性影响。

可以采用的方法如机器学习、大模型语义理解等技术。

3. 上下文理解

单独分析某一个字段，有时无法准确确定其真实含义，因此需要结合数据上

下文进行综合判断。核心作用是将数据内容、元数据和业务语境结合起来，提高数据语义识别的准确性。

上下文通常包括表名、字段名、字段注释、相邻字段、表间关系、数据结构、业务系统、数据来源等。

5.3. 安全分析层

安全分析层提供的是数据一旦发生泄露、篡改、破坏、滥用等安全事件，可能产生什么程度的影响。因为知道了数据是什么并不等于知道数据有多重要，安全分析是分级的重要依据。

1.重要性分析

重要性分析主要判断数据对于组织业务、核心业务活动以及相关主体的重要程度，是数据本身的重要程度。

分析因素包括数据涉及的业务范围、数据覆盖对象和规模、数据在业务活动中的关键程度等。

2.影响程度分析

影响程度分析进一步分析数据发生安全事件后可能造成的影响。本质上承担的是从内容属性向安全属性转化的分析过程。

可以从不同安全影响维度进行判断，如对个人、组织、社会及业务活动可能造成的影响、影响范围和影响程度等。

5.4. 分类分级层

分类分级层是整个技术体系的核心判定部分，负责根据前面的数据理解和安全影响分析结果，最终形成数据的分类和分级结果。

1.规则库

规则库用于承载分类分级所依据的标准、经验，分类分级引擎提供统一的判定依据。规则判定是速度最快、准确率最高的处理确定性内容的方法。

规则可以来自国家及行业相关标准规范、组织内部分类分级制度、特征规则、业务规则等。

2.分类引擎

分类引擎根据数据内容理解结果、元数据以及分类规则，对数据进行类别判定、标识。

其基本过程可以概括为数据内容/元数据、特征提取、规则或模型判断、分类结果。分类结果可以进一步以分类标签、分类属性或分类结果记录等形式进行保存和输出。

3.分级引擎

分级引擎根据数据分类结果以及安全影响分析结果，按照既定的分级规则确定数据安全等级。

分级的核心依据是数据属性+数据类别+重要性+影响程度+分级规则，与分类相比，分级更加依赖对数据安全影响的分析。

4.API 接口

API 接口负责将分类分级结果以标准化方式向外提供，解决的是分类分级结果如何被其他系统使用的问题。这也是分类分级产品从一个独立工具成为数据安全基础能力的重要接口。

输出内容可以包括数据资产标识、分类结果、分级结果、分类分级标签、相关判定信息等。通过标准化接口，可以将分类分级结果提供给数据安全管理平台、数据治理平台、数据安全防护系统、其他业务或安全系统。

5.5. 安全映射层

安全映射层负责建立分类分级结果与安全保护要求之间的标准化关联，通过分类分级结果和不同来源的安全要求生成对应的具体安全控制。

需要特别强调，这一层的定位不是直接实施安全措施，而是建立分类分级结果与安全保护要求的标准化映射关系，为后续差异化保护提供依据。这也使分类分级结果能够进一步被数据安全管理和具体安全防护能力使用。

1. 法律法规映射

根据适用的法律法规、标准规范等合规要求与相应的数据分类分级结果关联，建立对应安全控制。

2. 内部规章映射

将组织内部的数据安全制度、管理规范、数据管理要求转化成与分类分级结果对应的安全控制。

3. 业务风险映射

结合业务场景及业务风险要求，将分类分级结果转化成相应的安全控制。从具体业务风险出发，形成适配、准确的保护措施。

5.6. 人机协同技术

人机协同是内容理解、安全影响分析和分类分级判定的核心技术辅助。

随着大模型和人工智能技术应用于数据分类分级，系统可以利用大模型提高数据识别、语义理解和分析效率，但由于数据业务语义复杂、规则存在例外以及模型无法保证绝对正确，因此需要建立人机协同机制。

1. 大模型辅助

大模型主要承担提高数据理解准确度和分析效率的任务。

注：虽然有些数据安全分类分级工具采用大模型完成了全流程工作，但这种方式受限于数据资产规模和风险偏好，并不适用于所有企业。

大模型可进行字段语义理解、数据内容识别、上下文分析、分类辅助判断、分级辅助判断、复杂业务场景分析等。

2. 置信度评估

对模型或自动化规则产生的识别和判定结果进行置信度评价，可以把人工力量集中到真正存在不确定性的对象上。

通常采用高置信度结果自动通过，中低置信度结果进入人工确认的方式。

3. 人工审核

人工审核结果可以进一步反哺规则库和模型，使系统形成自动识别、置信度评估、人工审核、规则/模型优化、再识别的持续优化机制。

人机协同的核心不是简单地加入人工审核，而是利用机器扩大识别和分析能力，以人工保障复杂场景下的准确性和结果责任。

人工审核通常面向低置信度结果、规则冲突、模型无法判断的数据、复杂业务场景、重要分类分级结果等。

第6章 最佳实践

6.1. 运营商数据安全分类分级案例

6.1.1. 项目背景

数字经济时代下数据成为核心生产要素，电信运营商作为关键信息基础设施运营者，承载着海量用户数据与业务数据，面临《数据安全法》《个人信息保护法》等法规的刚性合规要求。某运营商是区域通信服务主体，业务覆盖移动通信、家庭宽带、政企专线与云网融合等全业务领域，网络规划、工程建设、运行维护与客户服务等核心业务系统长期运行，积累了 PB 级数据资产。其中非结构化文件型数据占比持续攀升，广泛分布于文件服务器、对象存储与办公系统中，隐含大量敏感个人信息与重要数据，数据安全管控压力持续加大。

为提升数据资产规范化、精细化管理，自 2025 年以来，该运营商依托大模型开展数据分类分级智能化升级实践，推动数据分类分级由传统人工抽检向全量自动化识别、智能化精准分类转型，有效提升数据安全治理与数据资产运营效能。

6.1.2. 需求描述

该项目启动前，该运营商在数据分类分级上面临四类现实困难：

1. 数据资产底数不清：数据分布零散、类型多样，缺乏统一的自动化盘点手段，难以形成可查询、可追溯的资产台账。
2. 非结构化数据识别失效：传统基于关键词与正则表达式的分类方法，对规划建设方案、测试验收报告、运维日志、应急通信保障预案和报告等文件型数据识别准确率低，成为最大的覆盖盲区。
3. 合规要求刚性：需同时满足《网络安全法》《数据安全法》《个人信息保护法》等法律法规对个人信息与重要数据的保护要求，并具备可自证的合规证据链。
4. 人工定级效率受限：依赖人工审核与定级，耗时长、成本高、标准不统一，

难以适应数据的动态变化。

6.1.3. 整体解决方案

项目立足运营商数据治理痛点，确立“AI 驱动、精准识别、动态治理”的总体建设思路，采用分层解耦、云原生化的架构设计，自下而上构建数据采集层、智能分析引擎层、能力服务层、应用展示层、安全策略联动层五大核心层级，实现资产从发现、管理到智能定级与态势呈现的贯通。



AI 赋能数据分类分级系统整体架构

1. 数据采集层：通过广泛的适配器，支持从关系型数据库、大数据平台（如 Hadoop、Spark）、文件服务器、对象存储等多种数据源进行非侵入式的数据采集和流量镜像。
2. 智能分析引擎层：为整套系统核心算力与决策中枢，包括多模态识别、AI 模型库、知识图谱及策略管理模块，为上层数据分类分级、风险研判、安全联动管控提供核心智能支撑。
3. 能力服务层：以 API/SDK 的方式，将数据识别、定级、风险评估等核心能力封装成服务，供上层应用和第三方系统调用。
4. 应用展示层：提供统一的管理控制台，实现数据资产地图、分类分级结果可视化、风险评估报告、运维监控看板等功能。
5. 安全策略联动层：通过标准接口与现有的数据防泄漏、数据库审计等安全产品对接，实现安全策略的自动下发与执行。

6. 在识别链路上，方案采用“三级递进”策略——字符级特征规则匹配、NLP 语义识别、LLM 大模型智能推荐，逐级消化前一级未能匹配的元数据，使 AI 能力精准作用于规则方法的失效区间。

6.1.4. 核心 AI 分类分级能力

1. NLP 语义识别与大模型智能推荐

项目将识别任务拆为三级流水线，对数据识别任务进行分层拆解、逐级穿透处理：

第一级，特征规则匹配。依托标准化分类分级策略库，以表名、列名、列描述、列取值、文件名、文件内容、应用接口名与参数名匹配分类分级策略中的数据特征规则，开展精准规则匹配。经实测，本轮元数据匹配率可达 80%。

第二级，NLP 语义识别。对列名称、列描述、文件名、文件内容、参数名称与参数说明做语义相似度识别，设置 85%相似度判定阈值，有效识别缩略语、外语与相似表述。

第三级，LLM 大模型推荐。针对前两级仍无法匹配的疑难元数据，依托大模型开展智能推理定级，对列名称、列描述、参数名称、参数说明自动匹配数据特征名称，文件名、文件内容自动匹配分类名称，完成复杂非标文本的兜底识别，彻底打通传统技术的识别盲区。

三级递进后，元数据匹配率由 80%提升至 98.84%，显著解决了传统分级覆盖不全、识别不准、效率不足的行业痛点，实现了 AI 从“概念赋能”向可量化、可落地、可复用的能力跃迁。

2. 知识图谱驱动的动态风险识别

项目在识别之外引入动态知识图谱，将数据实体、系统资产与用户行为构建为关联网络，并通过实时事件流持续生长。基于路径查询、社区发现与中心度分析，系统能够发现聚合风险，针对分散在各类文档中的员工姓名、所在部门、项

目奖金等单一敏感度较低的字段信息，传统静态分级模式无法识别关联风险，而知识图谱可捕捉用户高频关联访问的异常行为链路，对多维度低敏信息聚合形成的高风险场景自动触发安全告警，实现数据安全治理从静态固定定级向动态关联风险研判、主动预警管控的转型升级。

3. 面向 14 项目标数据项的专项识别能力

体系面向敏感个人信息 5 类 5 项（人脸信息、残疾人和军人身份信息、基于账户信息产生的支付标记信息、行踪轨迹和精确定位、身份证照片）与重要数据 4 类 9 项（网络规划建设、网络运行维护、网络与数据安全保障、应急通信保障相关文档）建立专项识别能力，覆盖规划建设方案、测试验收报告、监测分析数据、IP 地址分配信息、重大网络与数据安全事件报告、应急通信人员与设备储备情况等典型文件，共形成 9 类 14 项可度量的 AI 识别数据项。

4. 多模态语义理解与小样本自进化

针对通用大模型“看不懂行业黑话”的问题，项目以工单记录、运维日志、设计文档、应急预案等业务语料开展领域自适应微调，使模型掌握运营商术语体系与表达习惯；同时融合 NLP 引擎与 OCR 引擎，对扫描型 PDF、图片水印、截图与证件照片统一文本化，对压缩包与嵌套文档递归展开、对长文本按语义切片并行推理，实现从“字符匹配”到“语义认知”的跨越。

5. 关键性能指标

- (1) 处理规模：支持 PB 级数据存量扫描与 TB 级日增量处理，日处理文档超百万份，兼容 20 种以上常见非结构化文件格式与 16 种数据库类型。
- (2) 识别准确率：整体数据分类分级准确率大于 85%；敏感个人信息与重要数据识别准确率大于 85%；身份证、手机号、银行卡号等典型个人敏感信息识别准确率大于 90%。
- (3) 处理效率：相比传统人工方式，数据分类分级效率提升 50 倍以上，人工审核成本降低 60%。
- (4) 系统响应：API 平均响应时间小于 3 秒，支撑业务系统在线调用。

6.1.5. 应用成效与客户收益

本案例构建了多层次、立体化的智能化数据治理体系，以“领域大模型微调与多模态识别”夯实语义理解底座、以“三级递进识别流水线”打通规则与大模型的协同链路、以“动态知识图谱”发现聚合访问的隐性风险、以“14项专项识别”覆盖敏感个人信息与重要数据，将数据分类分级从基于关键词的机械性合规任务，升级为基于上下文理解的认知性智能活动，形成“识别—一定级—防护—监控”的运营闭环。既实现企业数据安全治理能力的迭代升级、长效演进，也为基础电信行业及各类大型数据持有方，提供了可复制、可落地、可量化、可演进的数据分类分级智能化治理实践路径，具备良好的行业示范与推广价值。

1. 数据资产底数由模糊转可视化、精细化：全网全域数据资产自动化扫描，动态构建可视化数据资产地图，形成可查询、可追溯、可动态迭代更新的非结构化数据资产台账，实现数据资产底数全景可视、全程可控。
2. 人工投入显著下降：依托大模型推荐与语义识别，大幅减少人工甄别、手动定级等重复性工作，有效规避人工操作偏差，整体人工审核成本降低 60%，实现数据分类分级工作降本、提质增效。
3. 合规举证效率跨越式提升：一键生成覆盖全量资产的分类分级图谱、个人信息清单与合规性报告，证据链完整，合规举证周期由原先数周压缩至小时级，极大提升合规自查与迎检工作效率。
4. 数据要素合规流通：清晰的分级标签为内部数据共享提供信任基础，敏感数据集自动施加审批与安全策略，实现数据“可用不可见”。



本案例选自天融信真实项目

6.2. 银行数据安全分类分级案例

6.2.1. 项目背景

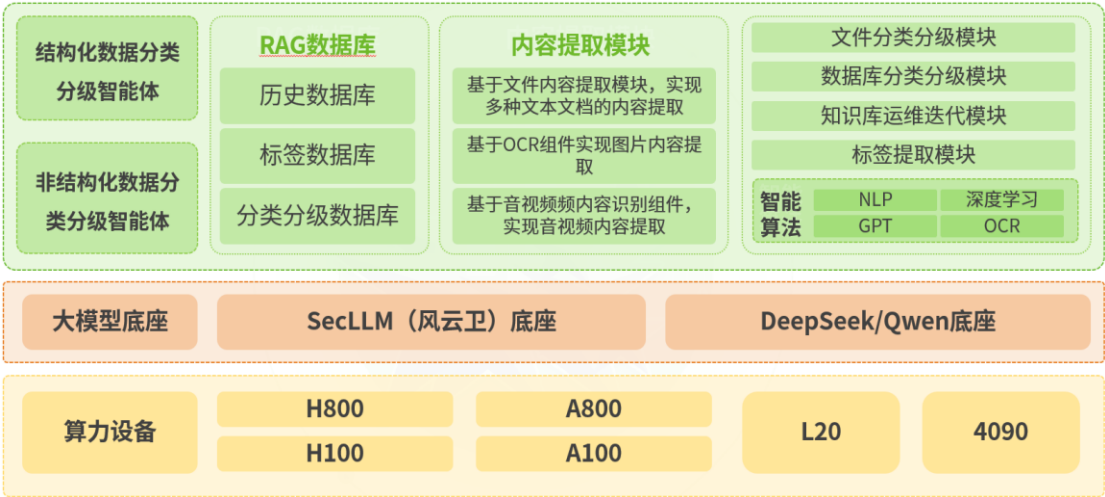
某银行拥有多源异构数据资产，涵盖客户信息、账户资金、交易流水、信贷风控、理财资讯等结构化数据。传统分类分级依赖正则、关键词匹配与人工复核，存在明显短板，隐性敏感字段识别不全、误报漏报率高、难以理解金融业务语义、数据表治理效率低，无法满足《数据安全法》《个人信息保护法》及金融行业数据分类分级指南的合规要求，也难以支撑精细化的数据安全防护与数据资产运营。为此，引入垂直大模型+RAG 知识库架构，建设数据分类分级治理体系，将数据梳理、分类、分级与迭代优化纳入统一流程。

6.2.2. 建设痛点

1. 金融数据业务复杂度高，大量隐性敏感字段无法通过传统规则识别，仅能识别身份证、手机号等强规则字段，或字段名、字段备注规范的字段；
2. 数据表关联关系复杂，同一敏感属性跨多表分散存储，人工梳理耗时大、准确率低；
3. 传统工具缺乏业务语义推理能力，难以结合金融场景判断数据风险等级，分级标准不统一；
4. 识别结果无证据留存、不可溯源，无法满足监管审计与自查报送要求。

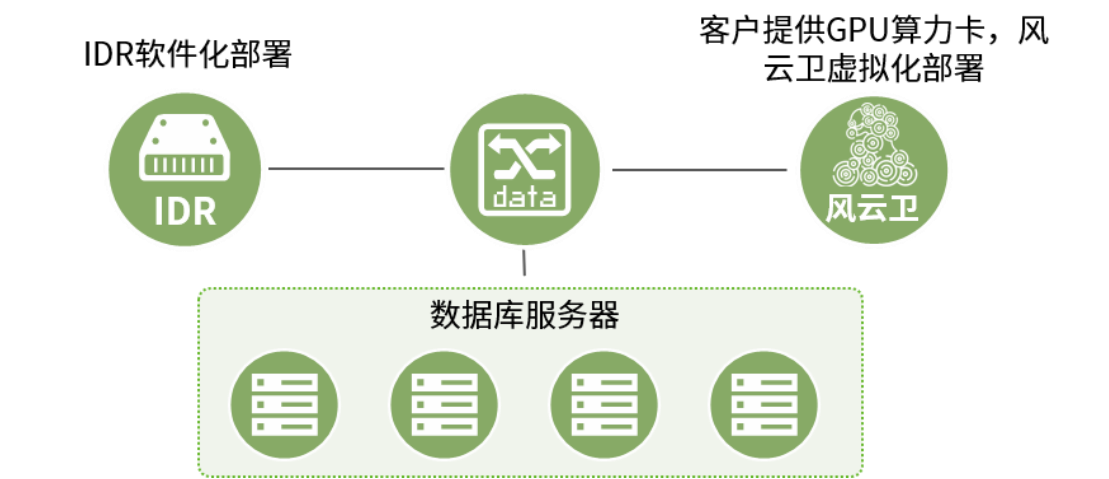
6.2.3. 整体方案设计

本项目借鉴 AI 智能体专家推理范式，在规则匹配的基础上引入大模型语义推理+金融 RAG 知识库+双模型交叉校验+证据留存的分类分级方案。依托大模型理解业务场景、数据表结构、字段语义与业务关联关系，补充传统固定规则的不足；同时引入双大模型交叉验证机制，降低单一模型误判，提升识别准确率。



平台内置金融行业标准分类分级知识库，可导入金融数据分类分级规范、个人信息判定标准，并结合历史人工复核样本持续迭代。识别流程覆盖资产自动扫描、字段语义推理、敏感属性判定、是否个人信息判定、业务类别判定、安全等级评定、证据留存、人工复核闭环等环节。

部署环境中，客户提供 GPU 等虚拟化环境部署 IDR 与风云卫；数据库采用客户提供的国产化数据库，中间件采用宝蓝德。



6.2.4. 核心落地能力

1. 金融语义智能识别：不局限于字段名称匹配，结合表注释与业务场景，识别客户隐私、账户信息、交易数据、信贷敏感数据等资产。
2. 一次任务出多个模板结果：支持在一次扫描任务中同时选择多个分类分级模

板，扫描完成后同时生成所选模板的结果，并在同一界面展示。

3. AI 聚类批量打标：基于语义与特征自动聚合相似字段，建立统一基准；对同簇数据一键配置标签，减少逐行手动操作，压缩人工复核频次。
4. 双模型交叉校验：支持风云卫与第三方大模型对数据进行分类分级，通过双向判定、结果比对纠错，降低人工复核工作量。
5. 标准化分类定级：按金融行业规范，同时完成多模板的分类分级，适配监管报送标准。



6. 全流程证据溯源：每条分类分级结果留存字段样本、推理逻辑与打标记录，可举证、可审计、可追溯。
7. 治理闭环：人工修正结果自动回流知识库，后续识别参照更新后的样本，复核工作量逐步下降。分类分级的准确度依赖对客户自身业务口径的理解，这部分知识无法只靠大模型获得。平台通过 RAG（检索增强生成）将人工复核经验沉淀为可检索的知识库，使模型在识别时参照该客户的历史判定结果。主要有：

- (1) 知识自动沉淀：人工复核确认的分类分级结果自动同步进入知识库，无需额外整理。每条知识记录字段信息、判定结论与来源模板。
- (2) 向量检索与样本注入：知识条目经模型向量化后存入向量数据库。执行分类分级任务时，先按当前字段语义检索出最相似的历史样本（few-shot 示例），再连同业务规则一并注入大模型提示词，使模型判断向客户既

有口径靠拢。

- (3) 按模板隔离：每个分类分级模板在向量库中对应独立的集合，不同模板的知识互不干扰，可分别维护与迭代。
- (4) 两种知识库服务模式：本地模式使用平台自带的向量库，数据不出内网；风云卫模式复用客户已有的风云卫知识库服务。两种模式在前端可配置切换。
- (5) 历史数据批量导入：支持将客户已有的分类分级成果（历史台账、其他平台导出结果等）批量导入知识库，使平台上线初期即具备一定判定基础，不必从零积累。大导入量场景下分批提交并支持并发处理。
- (6) 状态可查询、可启停：知识条目的同步状态、来源模板与更新时间可查询；知识库开关在前端可配置，方便启停。
- (7) 成果标准化输出：分类分级结果可通过 API 供资产管理平台、安全防护设备调用，形成统一标准。

6.2.5. 落地成效与价值

- 1. 建立了数据资产分类分级的管理机制与规范流程，形成标准化、可复用的分类分级测绘能力，可动态维护应用数据资产目录与地图。梳理工作由人工逐条处理转为系统批量处理，敏感数据漏报、误报问题得到改善。
- 2. 标准化、可溯源的分类分级结果，满足等保、数安法及金融行业监管自查与报送要求。结果可输出至客户的数据资产管理平台发布，并将数据安全要求纳入信息系统开发生命周期。分类分级标签可联动数据脱敏、访问审计、权限管控，形成差异化防护，降低敏感信息泄露与交易数据滥用风险。
- 3. 提升了数据服务的有效性与可用性。面向数据流通应用场景建立分级管控体系，在保障数据安全的前提下提升利用效率，同时减少人工梳理的人力投入。



本案例选自绿盟科技真实项目

第7章 产品与服务市场分析

7.1. 市场总览

1.数据安全分类分级产品与服务 2025 年市场规模约为 2.5 亿元，约占数据安全领域收入 3.6%。调研厂商中，收入中位数约 1000 万元。年收入高于 2000 万元的占比约为 29%。

2.合规为第一驱动，数据要素市场化/数据资产化为长期需求，"合规刚性+要素化长期价值"双重驱动格局清晰。

3.现阶段有关数据安全分类分级的项目中，数据安全分类分级产品和服务为直接需求的占比为 47.9%，并且这一数字表现出持续且强劲的上升趋势。这说明，越来越多企业不再只是为了完成某一个脱敏、加密或合规项目而开展分类分级，而是开始将其视为一项需要长期建设和运营的数据安全基础能力。

4.技术竞争焦点集中在非结构化识别与大模型落地，非结构化/多模态数据识别精度为技术难点，大模型落地的幻觉、成本与可解释性难题是亟需攻克的方向。

5.落地的最大障碍不在技术而在组织，最大困难指向数据底数不清、资产台账缺失，跨部门协同与权责不清等问题。

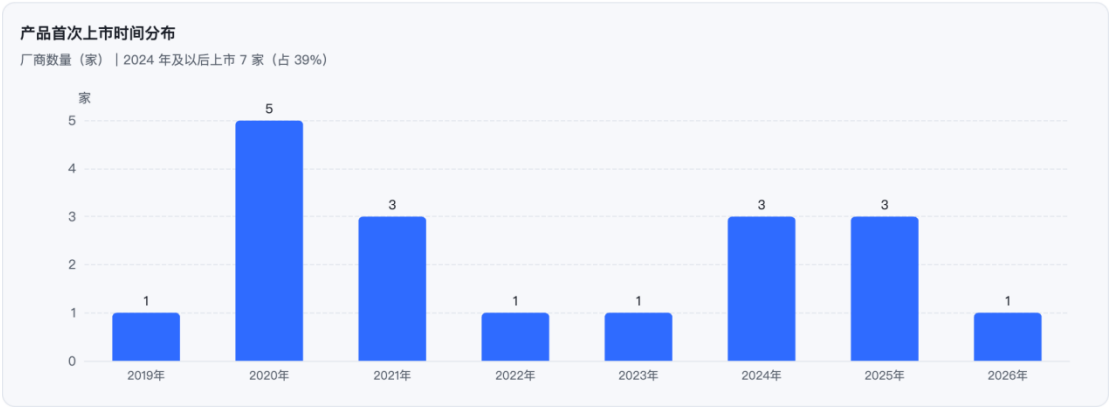
6.行业与区域收入集中度高，其中运营商(23.3%)、政府及公共部门(21.7%)、能源(21.5%)、金融(14.3%)，四大行业合计约 80.8%；区域上，华北(36.0%)加华东(31.7%)合计约 67.8%。

注：由于各供应商对于数据安全分类分级产品并未形成统一的划分标准，其收入被包含在数据安全治理、敏感数据识别等产品或方案中难以清晰剥离，只有小部分供应商可以单独统计收入。

数世咨询认为，对于本次调研来说，各供应商所提供的数据可能存在偏差，并且修正的难度较大。本着求真务实的态度，本次调研所涉及的收入数据仅供参考，

不建议作为决策的关键数据引用。

7.2. 产品与服务上市时间

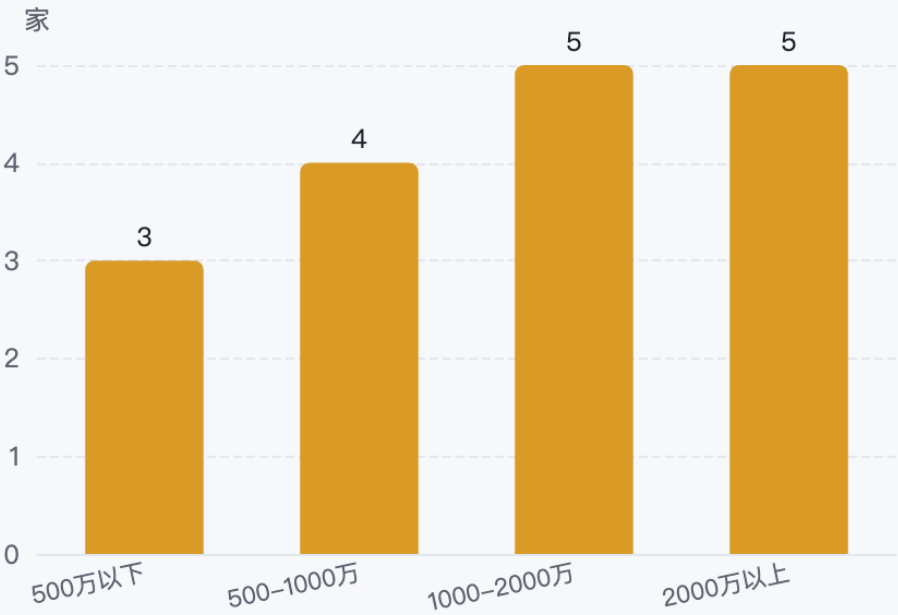


7.3. 市场规模



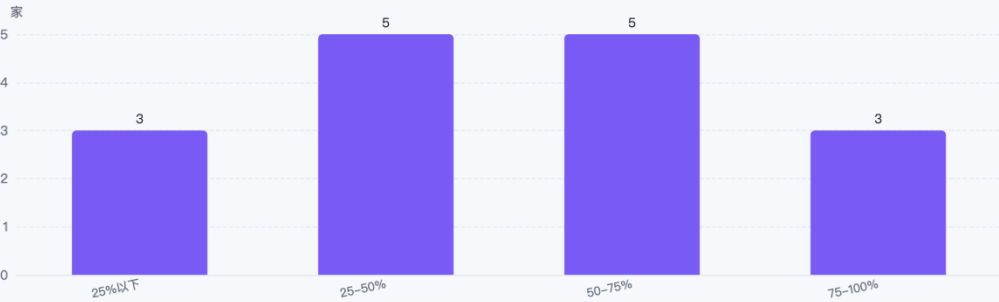
2025 年收入规模分桶

厂商数量（家） | 5 家（29%） 年收入在 2000 万元及以上



直接需求占比分布

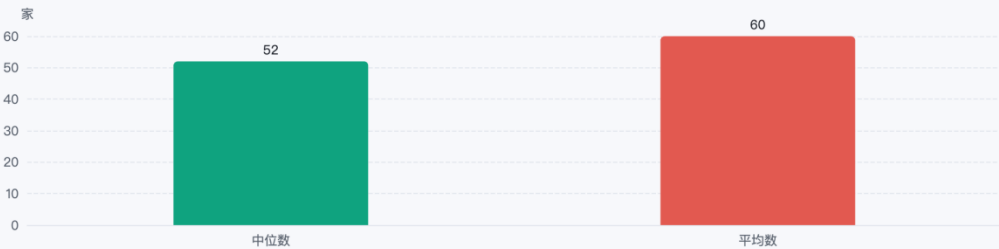
厂商数量（家） | 16 家填报，均值 47.9%、中位 45.6%



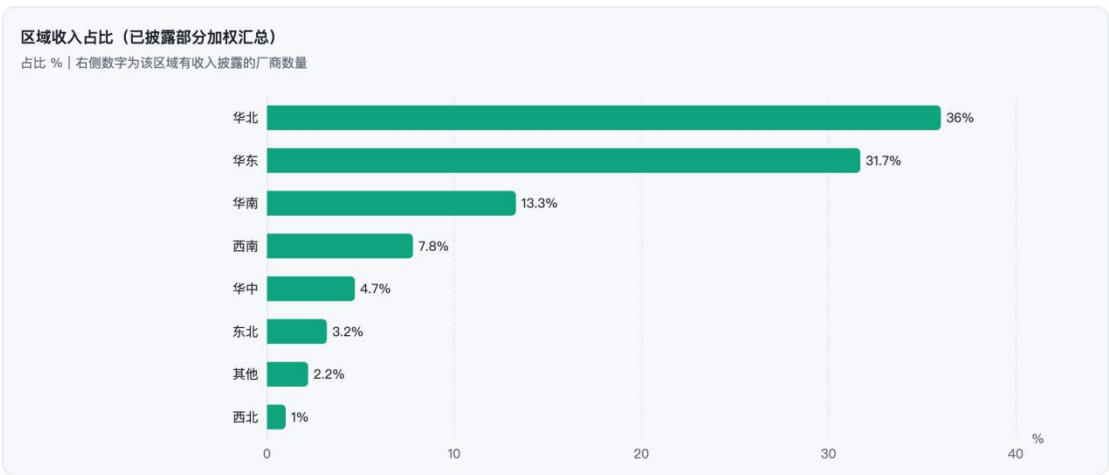
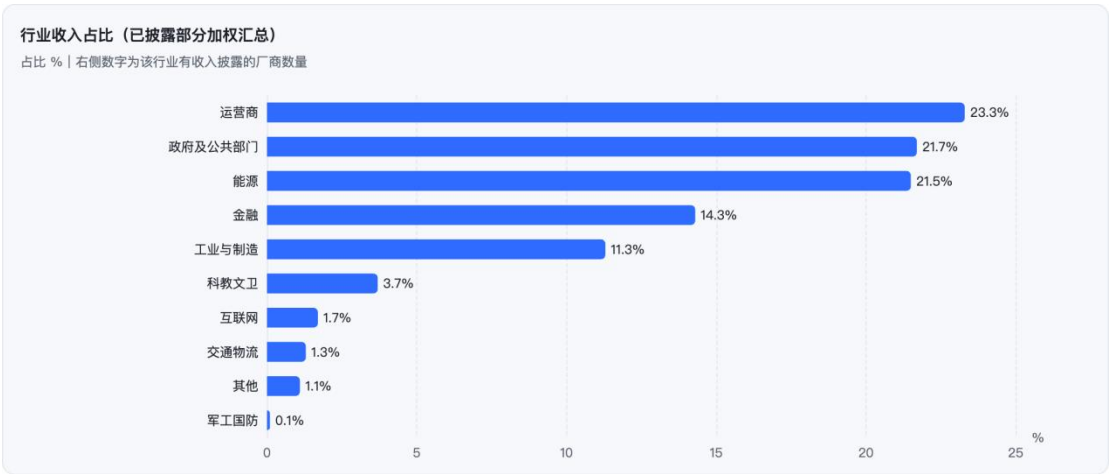
注：直接需求是指合同名称或项目实际内容是数据安全分类分级产品与服务，并非体系类、集成类建设项目。

客户数量：中位数 / 平均数

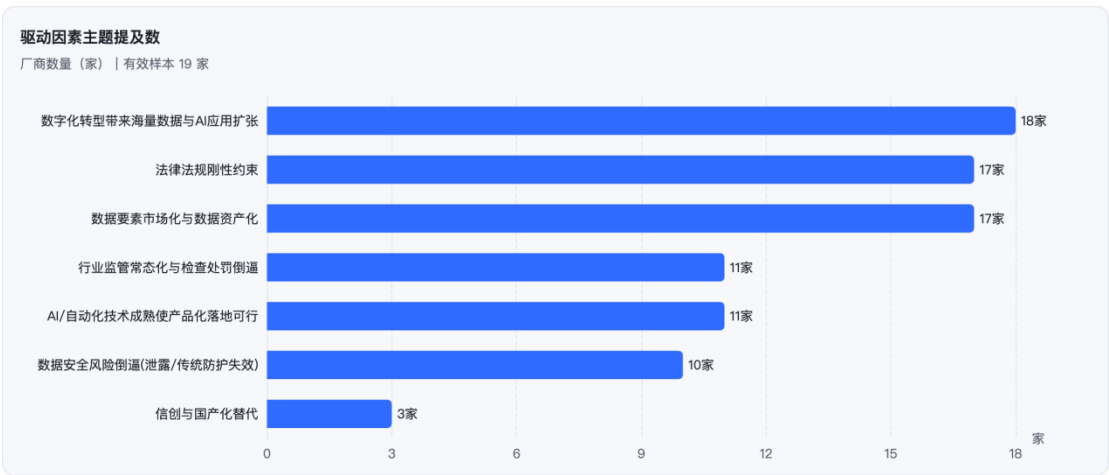
客户数量（家） | 14 家披露，合计 842 家



7.4. 行业区域收入



7.5. 驱动因素



7.6. 技术与落地难点



第8章 发展趋势

数据安全分类分级将逐步由数据识别与静态分级，向动态风险智能研判转变，实现从合规驱动的基础安全管理向风险驱动的精细化安全治理，最终向支撑数据安全流通和价值释放演进。

8.1. 短期：强化大模型内容识别

传统数据安全分类分级的核心问题其实不是分类分级的效果，而是系统是否真正理解数据。

比较通用的方法是根据字段、关键词、规则库来匹配数据类型，这种方法高效但存在较多的应用限制。随着数据越来越复杂并且体量越来越庞大后，仅靠字段与规则匹配往往会遇到很多困难，不能区分实际意义。这就迫使数据安全分类分级需要从字段识别转向内容理解。

利用大模型强化内容识别能力，不是简单替代规则匹配，而是形成规则与模型协作的识别体系。因为大模型的价值并不在于识别的更多，而是能理解并区分实际意义。

数据内容理解包括敏感信息识别、数据类型识别、业务语义理解、数据主体识别、数据用途理解、数据上下文理解、数据关系理解等。虽然现阶段大部分企业对字段下数据的分析持谨慎态度，但大模型仅通过对业务系统、字段、字段间关系的分析也会极大提升数据安全分类分级的准确率。

相信随着数字化业务的发展以及安全能力的提升，会有更多的企业选择开放字段下数据的分析权限，通过大模型赋能的数据安全分类分级将真正实现完全自动化。

8.2. 中期：智能化安全影响分析

安全影响分析解答数据的重要性以及出现安全事件所造成的影响，其价值在

于给出数据安全分类分级的精确依据，提升结果的科学性与可信度。

现阶段的数据安全分类分级通常采用典型的合规映射逻辑，即通过法律法规或规章制度的明确要求机械化的设置分级结果，如 1000 万人以上个人信息、100 万人以上敏感信息等。

但对于没有明确量化或模糊性要求，按照简单的数据类型加数量判断，可能很难真正反映其存在的风险，在现实中往往无法准确定级。因为影响风险的因素可能还有数据主体、数据规模、数据敏感程度、数据用途、数据所在系统、对外开放程度、是否跨部门共享、是否跨境等。

所以需要安全影响分析确保不同风险对应不同保护强度，实现合规之上的精确化安全管理。

其真正价值在于满足法规要求的基础上，根据实际风险进行差异化配置。因为法规解决的更多是底线要求，但企业真正需要处理的是数据真正的危险以及安全资源应该如何精准投入。

8.3. 长期：数据汇聚安全风险分析

数据流通的本质是有效使用数据，而除了单独使用外更多的是关联分析、汇聚分析，真正的价值源于流通、融合、分析、加工，例如医疗数据、人口数据、科研数据汇聚后可产生超越其自身的新价值。

这时需要解决的问题就是数据与其他数据汇聚后将会产生什么新风险，因为单条数据可能风险极低，但多个数据汇聚后可能产生较高风险。如“姓名+手机号+位置+消费记录”汇聚后将形成一个人的高度完整画像，被滥用后风险极大且可能威胁人身安全，这时安全风险就发生了较大的变化。

现阶段我们关注的是单条数据或单类数据本身的风险，未来将更多的关注到数据组合、关联、汇聚后产生的新风险，因为风险不再只存在于数据本身，而存在于数据之间。

主笔分析师信息



靳慧超（Anatole Jin）

数世咨询 · 战略分析师

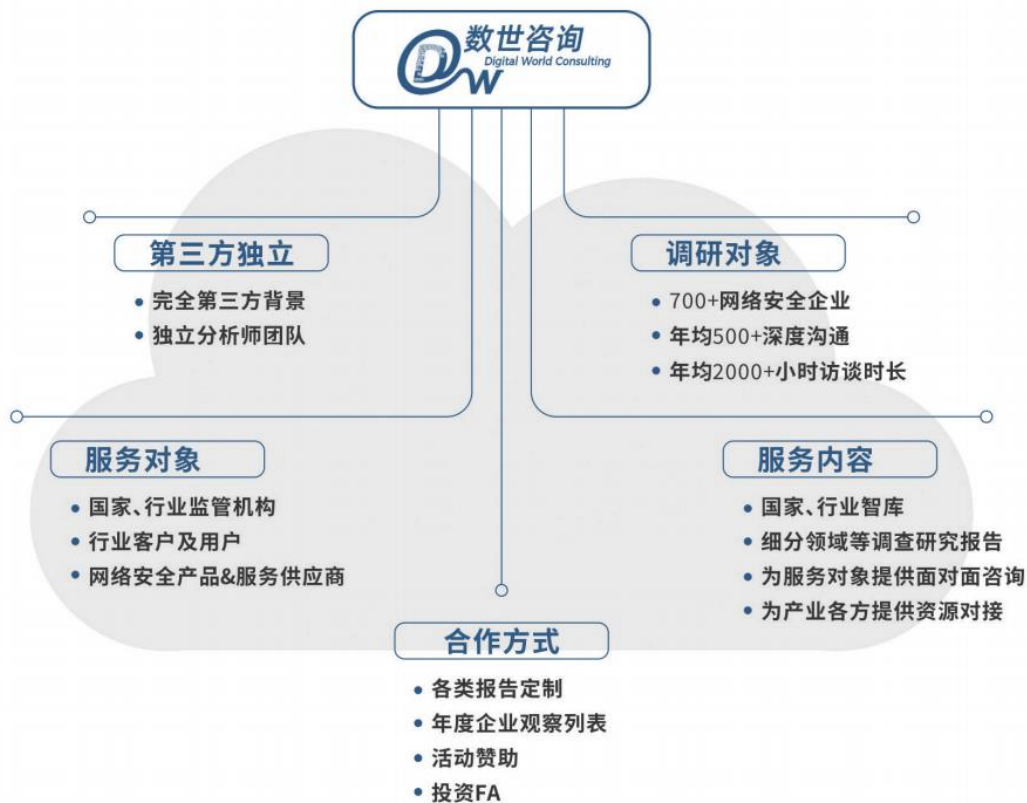
16601182683（微信同号）

添加时请注明“公司-姓名”

曾就职于神州数码集团-安全 BG、启明星辰集团-战略咨询中心、360 集团-城市产业事业部，主要负责安全咨询、规划等工作

现任数世咨询战略分析师、合伙人

研究方向为数据安全、AI 安全、软件供应链安全



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

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监管机构、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余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等。

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

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





数字安全领域独立第三方调研机构

数据安全 分类分级调研报告

