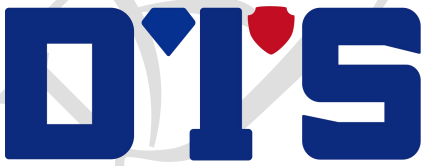
数达安全

数据资产管理系统白皮书



重庆数达信息安全技术有限公司

2023 年 11 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更新，恕不另行通知。

数达安全在编写本文档的时候已尽最大努力保证其内容准确可靠，但数达安全不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目录

1 引言

1.1 法规安全要求

1.1.1 数据安全法

第二十七条规定：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

1.1.2 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。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。（四）采取数据分类、重要数据备份和加密等措施；

1.1.3 个人信息保护法

第二十一条规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。（四）采取数据分类、重要数据备份和加密等措施；

1.1.4 《GB/T 22239-2019 等保 2.0》

8.1.10.2 资产管理，本项要求包括：

a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

1.1.5 GB/T 35273-2020 信息安全技术 个人信息安全规范》

3.2 中针对个人敏感信息提出一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

11.5 中针对数据安全能力提出个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

1.2 业务需求

1.2.1 行业发展需求

资产是个人或组织控制的有价值资产，企业资产有助于实现企业的目标。数据以及数据产生的信息已经被公认为是企业的资产。

离开高质量的数据，很难有企业仍然可以高效运行。今天，各企业都依赖于它们的数据资产以做出更明智和有效的决策。市场领导者正利用数据资产，通过丰富的客户资料、信息创新使用和高效运营取得竞争优势。企业通过数据资产，提供更好的产品和服务,降低成本,控制风险。随着企业对数据需求的不断增长，以及企业对数据依赖性的不断增强，人们可以越来越清楚评估数据资产的商业价值。

1.2.2 数据资产缺乏有效管理

每一个企业都需要有效地管理其日益重要的数据，通过业务领导和技术专家的合作，数据资产管理职能可以有效地提供和控制数据资产。

然而现实中，对数据资产的管理和应用往往还处于摸索阶段，数据资产管理面临诸多挑战。主要表现为以下几点：

企业内部工作人员对于资产登记备案多是以纸质化办公，随着公司规模的扩大，其拥有的数据资产也随之递增，这种传统的工作模式导致效率低下、资料保存查询困难、成本高、不利于多人协同办公，成为日常办公的严重制约。

数据资产存在着巨大商业价值，而多数企业存在资产分布不清、资产归属部门不清、敏感数据缺乏保护等问题，一旦出现数据泄露等安全问题，很难追责。

受限于数据规模参差不齐和数据源种类庞杂，多数企业的数据应用刚刚起步，

主要集中在精准营销，舆情感知和风险控制等有限场景，应用深度不够，应用空间亟待开拓。

大部分企业和政府部门的数据基础还很薄弱，存在数据标准混乱、数据质量层次不齐、系统间数据孤岛化严重等现象，阻碍了数据的共享应用。

随着公司内部信息化建设的完善，对业务流程梳理标准化、设备资源管控规范化、应急事件响应高效化都提出了新的挑战。而传统的数据资产梳理管理方式存在着管理流程不严、技术手段缺失、人员素质参差的问题，需要用专业的技术及产品来加以完善，这样可以提升工作效率，快速协调资源，规范管理流程。

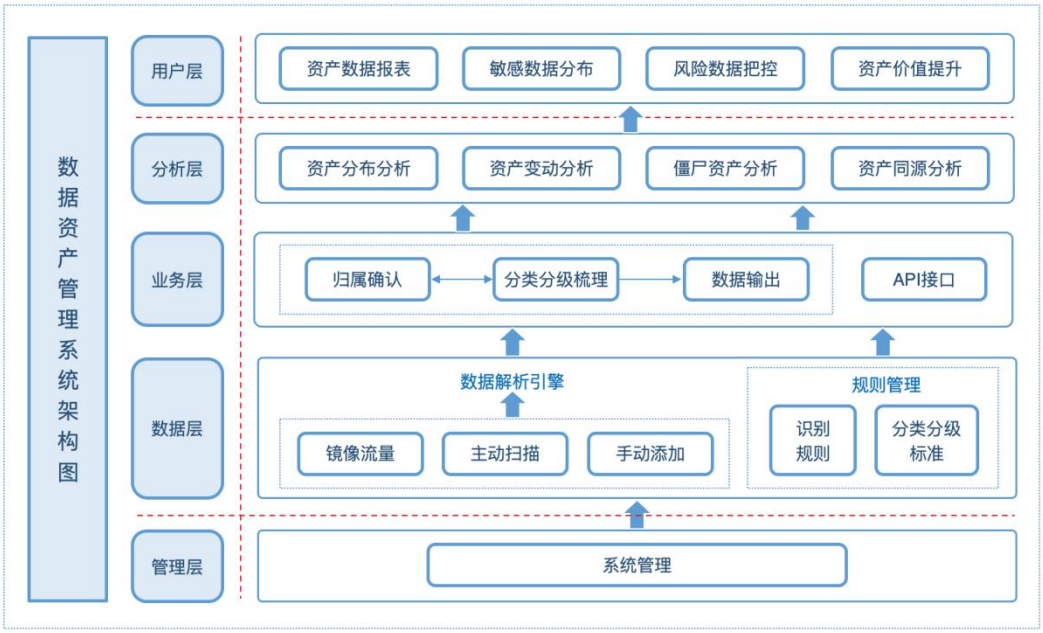
2 产品简介

数达安全数据资产管理系统（简称 DS-DAM）立足数据安全治理的起点和重要环节。系统以资产发现与资产梳理为核心、以资产可视与资产可管为目标，提升企业对数据资产的整体管控能力和运维效率。

DS-DAM 通过主动扫描方式与数据库协议分析，结合高效数据识别与可视化等技术，实现自动化数据分类分级及数据资产动态分析。提供相关接口以便快速打通安全链上下游能力，为全局性数据态势感知与数据精准差异化管控提供有效支撑。

3 产品架构

DS-DAM 架构主要包括管理层、数据层、业务层、分析层和用户层。



管理层以系统管理的业务监控、用户管理、系统诊断等内容为依托；

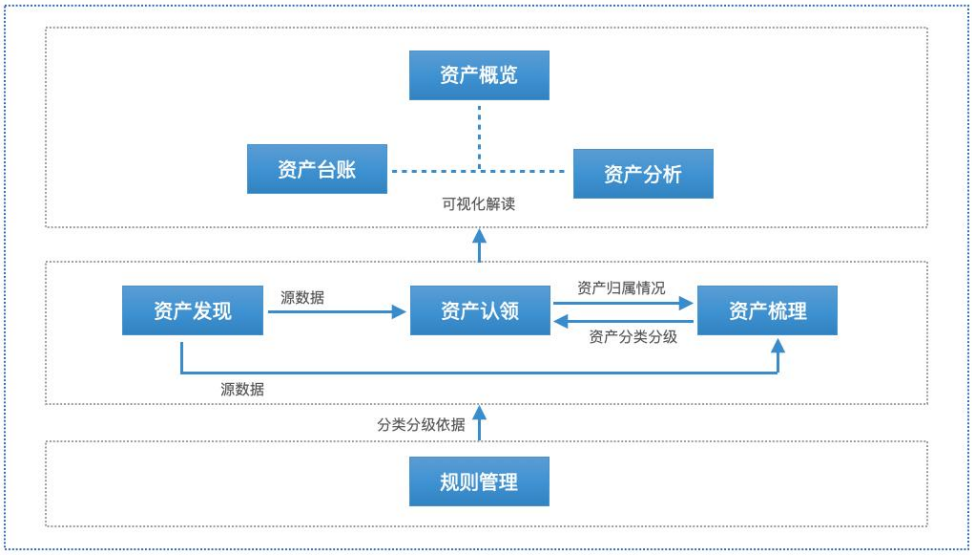
数据层以数据发现与解析、规则管理为基础；

业务层通过归属确认、分类分级梳理、数据输出、API 接口等业务处理；

分析层对资产分布、资产变动、僵尸资产和同源关系的进一步分析，最终能够帮用户理清数据资产，明确敏感数据分布，规避资产风险，提升资产价值。

4 产品功能

DS-DAM 功能主要包括资产概览、资产发现、资产认领、资产梳理、资产台账、资产分析和规则管理。各功能之间的业务关系如下：



功能业务关系图

4.1 规则管理

DS-DAM 提供敏感数据识别规则和数据分类分级标准的管理功能，为资产敏感数据发现与分类分级打标提供依据。

DS-DAM 内置敏感数据识别规则，包括地址、姓名、手机号、银行卡号、税号、营业执照编号等一百余项，支持通过对正则表达式、自定义函数、混合类型等匹配方式和匹配率的配置，构建丰富的特征项。提供对正则表达式的独立管理功能，包括系统内置和自定义数据，用于正则表达式匹配方式的配置。

DS-DAM 内置电信行业分类分级标准，用户可根据实际业务，通过自定义的多层级类别进行数据分类管理。数据分类支持敏感等级、描述和识别规则的管理，用户可对分类内容进行敏感定级，给分类添加规则标签，作为敏感数据的匹配依据。

4.2 资产发现

DS-DAM 拥有完善的资产发现方案，通过静态扫描、动态解析、手动添加等多种资产发现方式，能够自动发现数据资产的基本信息，包括：IP、资产类型、资产来源等，也为资产认领、资产梳理等功能提供了基础数据。

DS-DAM 支持通过指定 IP 段和端口范围，对网内数据库执行即时、预约、定期自动扫描任务；拥有资产动态发现能力，通过对数据库访问的镜像流量包的自动解析，持续发现新的数据资产；支持手动添加单个资产或通过文件批量导入，完善资产数据源。

DS-DAM 还支持对数据库账户进行鉴权，通过权限检查，保证基础数据的提供和后续业务的处理；同时拥有集群发现能力，通过内置规则对疑似集群进行检测和确认，加持资产数据分析的准确性。

4.3 资产认领

资产认领是对数据资产进行权责归属确认的过程。基于资产发现中已确认的数据资产，将资产以模式(库)的维度指认给相应的资产所有者。

用户可通过手动添加或文件导入的形式，建立多层级的资产所有者组织架构。将未认领资产指认给所有者之后，相应所有者或所属组织架构下即可查看到所拥有的资产信息。

4.4 资产梳理

资产梳理是以资产发现中已授权的数据资产为基础，依据规则管理预定义的敏感数据识别规则和数据分类分级标准，对资产的内部数据进行自动随机抽样，识别解析，发现敏感数据，并对敏感数据进行分类分级打标的过程。

用户能够预设资产梳理任务所依据的分类分级标准、梳理范围、采样量、匹配率和错误处理等，对数据资产进行单条或批量梳理。系统支持查看梳理进度，同时支持对资产的梳理配置进行调整和重新梳理，系统对资产分类分级的统计分析则是依赖于对资产最近一次的梳理结果。

4.5 资产台账

DS-DAM 结合资产发现、认领和梳理的处理结果，对全局资产数据进行输出。提供了多维度的数据资产专项统计数据，包括资产清单、分类分级和资产归属等供用户分析审核，能够帮助用户对所拥有的数据资产进行全面了解。

用户可将不同维度的资产数据台账进行导出，以满足离线查看、分析汇报等使用场景，也可作为基础数据对接到其他系统平台。

DS-DAM 还支持用户查看资产梳理结果详情，并对敏感数据所命中的敏感规则进行核查和调整，实现敏感数据的精准识别。

4.6 资产分析

资产分析可以帮助用户从海量的数据资产中快速明确敏感数据分布，了解资产变化动态，评估资产潜在风险，以确保能及时掌握资产数据的安全状态并制定相应的防护方案。

资产分布分析：将资产归属、业务系统、敏感分类分级、资产地图等资产属性，通过可视化图表进行联合解读，可以清楚地了解到不同归属、系统和敏感等级下的资产数据所涉及敏感分类的统计信息，掌握数据资产具体分布情况和不同维度的关联关系。

资产变动分析：系统执行对资产新增表、删除表、表结构变更、数据迁移等变动信息的定时监控任务，并以可视化图表形式进行统计分析，同时能够支持查看资产最新变动动态。

资产风险分析：对僵尸资产和资产同源关系的统计分析。僵尸资产依赖于访问行为审计数据的支持，用户可以了解到不同时间周期，未被访问资产的分布情况；同源分析则是根据前置的分析规则、分析范围和匹配率，对设定的目标表的同源关系进行检测和分析。

4.7 资产概览

DS-DAM 将资产统计、资产变化趋势、涉敏资产变化和资产归属分布等多维内容，通过可视化图表的形式，将数据资产的总体状态进行了集中展示，能够使用户对资产的当前状态一目了然。

5 产品价值

智能发现、资产清晰：资产自动发现，解决资产不清、管理繁琐、效率低下等问题；

敏感定位、安全可控：敏感数据发现，分类分级打标，避免敏感数据不明导致的数据泄露、黑客攻击等安全问题；

资产到人责任分明：资产认领，应对资产权属混乱的现状，防止数据资产权

责不明导致的违规操作、资产混乱等问题；

风险可视、规避隐患：资产变动分析，便于发现资产变化中的异常操作，及时处理；僵尸资产和资产同源关系的分析，便于发现资产内部潜在的风险，及时规避；

安全能力协同：API 接口支持，支撑资产内部数据的多渠道和多场景应用，提升资产利用价值。

6 产品优势

6.1 强大的资产发现能力

- 多种资产发现方式的组合应用，能够最大程度地提高资产发现能力；
- 流量动态监测，可持续发现新的资产，应对资产动态变化，避免资产遗漏；
- 资产扫描的即时或预约任务，可灵活应对不同发现场景；
- 集群发现能力，能够避免重复任务，保证资产数据源的准确性。

6.2 丰富的敏感数据识别规则

DS-DAM 内置多样化的敏感数据识别规则，支持多种匹配方式下的规则自定义扩展，如正则表达式、自定义函数、混合类型等。同时可自定义分类分级标准，满足各行业下对数据灵活识别的需求，使敏感数据识别和分类分级方案更贴合实际业务，实现对敏感数据的有效识别和分析，提高对敏感数据安全监控的准确性。

6.3 精细化的数据资产报表

DS-DAM 提供多维度的数据资产报表，以供用户审核分析。整合全局资产数据，以资产目录方式直观地展现，并能够通过检索条件迅速定位，能够清晰了解到资产的统计情况、数据明细、敏感分布和资产归属等信息。同时可生成报表文件，满足离线查看、数据分析、总结汇报等需求，方便资产管理者进行资产管理，全方位掌握资产组成及状态，为资产价值最大化提供保障。

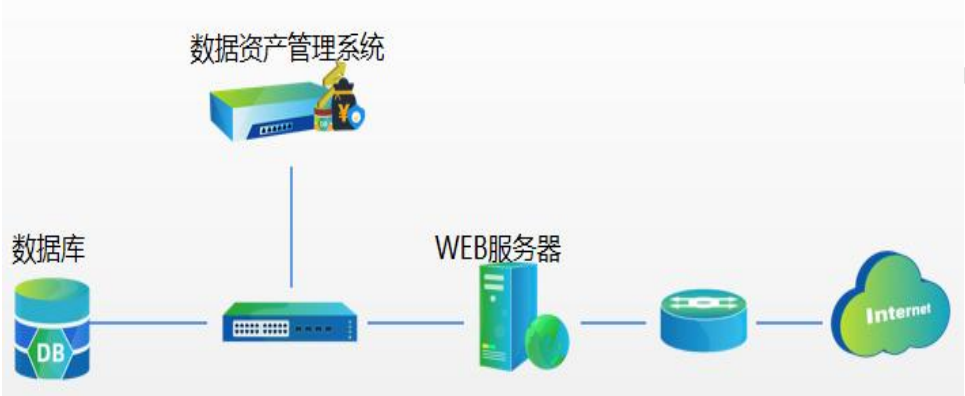
6.4 多维度的数据资产分析

DS-DAM 将资产归属、业务系统、分类分级等资产属性进行联合解读，便于用户对资产分布、不同维度关系的掌握。同时通过解析资产变化动态、分析僵尸

资产以及资产同源关系，不仅有助于发现资产潜在风险，也可助于发现资产数据结构问题，提升资产质量。

7 部署方式

DS-DAM 以旁路方式部署，通过直接连接数据库和流量镜像实现旁路监听。如下图所示，设备在交换机上将访问数据库的网口镜像到系统的业务网口上，系统通过分析镜像链路传过来的数据通信包，实现数据资产的发现功能。此种模式可完全独立于数据库部署，不影响数据库的正常使用。



旁路部署图示