数达安全

数据安全合规评估系统

产品白皮书

V2R0

重庆数达信息安全技术有限公司

2023 年 1 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

前言

近年来，以 5G 技术、数字化、智能化为主要特征的新工业革命蓬勃兴起，推动我国产业结构深刻变革。数据作为创新发展的基石，已成为国家基础性战略资源和驱动行业转型发展的重要引擎。随着全球数据呈现爆发增长和海量集聚，为人类带来无限发展机遇的同时也带来了新的安全风险和挑战，严重影响国家安全、经济发展、社会稳定和个人权益。

在此背景下，数据安全的重要性被提到了前所未有的高度。我国积极加强数据安全管理布局，《网络安全法》、《数据安全法》与《个人信息保护法》的相继出台，全面构筑了中国数据安全领域的基础法律框架。继上述三个国家级法律之后，各行业陆续出台了本行业配套的法规、标准、指南。为我国企业落实数据活动主体义务与责任提供了法律依据。

为解决目前部分企业在配套了防护能力后仍无法验证或利用人工等方式开展评估验证的局面，避免企业网络数据安全防护效果差、风险难发现等问题。数达安全按照国家政策、法律法规、行业监管等要求，以及对数据安全防护技术的深刻理解，构建数据安全评估体系，研发了数据安全合规评估系统，为数据安全评估体系提供技术评估手段，支撑企业全面提升数据安全防护能力。

1 背景

1.1 数据资源成全球博弈主赛道

在数字经济时代，信息和知识普遍以数字化的形式产生、保存、传播和利用，通过对数据资源的探索利用，可以推动更多新兴技术、新兴模式、新兴产业诞生和发展，推动传统产业转型升级。数据也因此成为新的生产要素和国家基础性的战略资源。

2022 年 4 月 10 日发布的《中共中央 国务院关于加快建设全国统一大市场的意见》中提出，加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。

数据网络空间成为了国家间博弈的新角力场，正在重塑全球政治经济格局。国与国竞争日趋多元化和白热化，在数据技术的加持下，政治博弈、经济角力、安全渗透都已是不容忽视的新的战争形式。

1.2 全球重大数据泄露事件频发

大数据、互联网、5G 的迅速发展，为人类带来无限发展机遇的同时也催生了大量的数据泄露事件，严重影响国家安全、经济发展、社会稳定和个人权益。

数据泄漏事件几乎覆盖国内外所有行业，全球各地深受数据泄露事件困扰的同时也造成了重大损失。

如：国外安全研究团队 Cyble 在一次日常安全监控中发现了多个帖子正在出售个人数据，与中国公民有关的记录总数超过 2 亿；被媒体称为“史上最大规模的数据窃取案”涉及 30 亿条用户数据，波及范围包括 BAT 在内的全国 96 家互联网公司；乌克兰媒体《乌克兰真理报》3 月 1 日在其网站发布了在乌克兰作战的 12 万俄罗斯军人的个人信息，详细记录了 12 万俄军的名字、注册编号、服役地点、职务等信息，页数多达 6616 页；《纽约时报》从 1200 多万人的电话记录中获得了超过 500 亿个位置的数据集，研究人员仅用了几分钟就对位置数据完成了反匿名处理，并获得特朗普一天的行踪记录。

1.3 数据安全面临的主要风险

数据全生命周期涵盖采集、传输、存储、使用、共享、销毁共六个阶段，其全生命周期都存在数据安全风险隐患的问题，针对数据全生命周期的技术防护是企业开展数据安全的核心和难点工作。以下为企业各个阶段的数据安全现状及存在的风险。

1.3.1 数据采集阶段

存在管理制度不规范、采集策略不合理、缺乏采集监控能力等，导致未授权采集、过度采集、采集质量低、数据倒流等风险。

1.3.2 数据传输阶段

存在重要数据未加密传输、缺乏数据流动监测、缺乏溯源手段等导致数据泄露和非法篡改的风险。

1.3.3 数据存储阶段

存在重要数据明文存储、数据备份与恢复能力不足导致数据泄露、丢失、无法复原的风险。

1.3.4 数据使用阶段

存在未建立数据访问控制机制和数据风险评估机制导致数据使用不当或恶意盗取、分析结果滥用的风险。

1.3.5 数据共享阶段

存在接口安全管控能力不足、数据溯源能力缺失、数据脱敏能力缺失，导致数据未授权提供、超范围公开、再转移等风险。

1.3.6 数据销毁阶段

存在销毁技术手段不完善、缺乏销毁管理措施导致残余数据利用和残余介质利用的风险。

1.3.7 共性安全风险

此外，企业因缺乏数据分类分级标准和实践造成关系国家安全、重要民生等核心数据的脱管和泄露、缺乏整体数据安全态势感知和数据安全检测评估能力导致企业无法对数据处理活动进行整体的监测预警和安全风险评估。因员工误操作、权限滥用、恶意窃取以及外部攻击等因素造成的数据安全事件等风险广泛存在数据的全生命周期各个阶段中，属于共性安全风险。

1.4 数据安全评估需求

1.4.1 数据安全合规要求

1.4.1.1 《网络安全法》

第二十一条：网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，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：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的 网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施。

第四十二条：网络运营者 不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

第五十九条：关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

1.4.1.2 《信息安全技术：个人信息安全规范》

《信息安全技术：个人信息安全规范》（GB/T 35273-2017），规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。针对各类组织的个人信息处理活动给出了具体操作规范，提出了个人信息安全保障明确要求：

1、传输和存储个人敏感信息时，应采用加密等安全措施。

2、涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜

对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。

3、对外提供学术研究或描述的结果时，应对结果中所包含的个人信息进行去标识化处理。

4、应建立自动化审计系统，监测记录个人信息处理活动。

1.4.1.3 电信行业数据安全规范

工信部 24 号令：电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十三条：电信业务经营者、互联网信息服务提供者应当采取相应措施防止用户个人信息泄露、毁损、篡改或者丢失：

对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施。

大数据安全指引要求：数据脱敏、数据加密、数据全面审计。

工信部保 368 号文：落实数据安全和用户个人信息安全防护标准要求，完善网络数据和用户信息的防窃密、防篡改和数据备份等安全防护措施。强化对内部人员、合作伙伴的授权管理和审计，加大违规行为惩罚力度。发生大规模用户个人信息泄露事件后要立即向通信主管部门报告，并及时采取有效补救措施。

1.4.1.4 电信和互联网企业网络数据安全合规性评估要点（2020 年版）

为进一步指导电信和互联网企业做好网络数据安全合 规性评估工作，提升数据安全保护水平，依据《网络安全法》 《电信和互联网用户个人信息保护规定》等法律法规，参考 《信息安全技术 个人信息安全规范》等标准规范，制定本 要点，供各企业在网络数据安全合规性评估中使用。

1、 基础性评估要点：重点围绕机构人员、制度保障、分类分级、合规评估、权限管理、安全审计、合作方管理、应急响应、投诉处理、 教育培训等十个方面开展评估。

2、数据生命周期评估要点：重点围绕数据采集、传输、存储、使用、开放共享、销毁等六个环节开展评估。

3、技术能力评估要点：重点围绕数据识别、安全审计、防泄露、接口安全管理、个人信息保护等五个方面开展评估。

1.4.2 业务安全需求

数据安全评估需依据相关数据安全合规要求，对信息系统及由其处理、传输

和存储的数据的保密性、完整性和可用性等安全属性进行评估。需提供以公用电信网和互联网网络单元以及业务系统中的数据为核心保护对象的、面向各种应用场景的数据安全评估。需要围绕着数据梳理和分类、存储加密、传输加密、权限管理、数据脱敏、日志审计、脆弱性管理、接口安全、数据防泄漏等要点展开。工具需支持以下维度的技术检测手段：**敏感数据识别、数据分类分级情况、数据加密情况、个人信息去标识化情况、数据操作日志记录情况、数据库账号安全情况、数据溯源能力、数据防泄漏能力、接口安全能力等**。

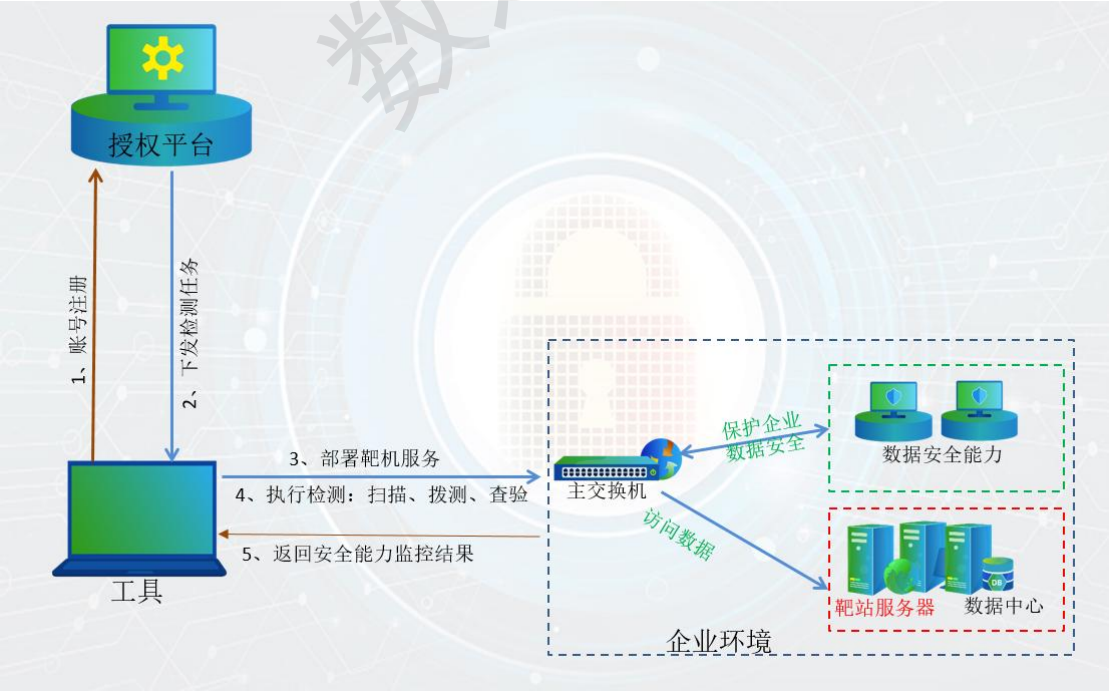
2 产品介绍

数达安全数据安全合规评估系统（SD-DPT），按照行业标准和规范要求，对数据安全防护技术的深刻理解，打造了一款具备多项技术检测能力的数据安全合规评估系统

2.1 产品目标

支持企业"自发性、周期性、专业性"开展数据安全技术能力合规评估，发挥合规性评估对企业数据安全保障水平的提高，解决了目前部分企业在配套防护能力后无法验证或利用人工等方式开展评估验证的局面，避免了企业防护效果差、风险难发现等问题。

2.2 产品原理



产品原理图

1. 授权平台提供账号与注册码，工具与授权平台网络可达的情况下，账号

在工具上进行注册账号。

2. 账号注册成功后，工具接入企业环境可直接进行检查。（工具与授权平台网络不可达也可使用）
3. 工具通过自动识别、模拟拨测、系统查验等方式进行检测：

1) 自动识别：内置敏感数据识别算法、新增敏感数据识别规则，通过扫描数据库的方式，自动发现敏感数据；
2) 模拟拨测：通过工具与靶站的交互，模拟拨测敏感数据访问行为，与企业反馈的数据安全能力监测情况进行比对，检查企业建设的数据安全能力情况；
3) 系统查验：查验企业的数据安全能力系统、被查系统，记录检测项的情况，生成相关的检测结果。

2.3 产品架构

产品架构图

客户端工具：检测能力重点对准影响数据安全风险防控效果的关键问题，从数据保护能力实施的完整性、有效性和准确性等方面进行评估评测和效果验证，服务检查，支撑监管。

靶站：单独的部署环境，隔离企业生产环境数据，为检查过程中模拟企业敏感数据存储，为企业敏感数据风险访问行为提供接收服务。靶站服务包含：MySQL、HTTP、FTP 等服务。为客户端工具的接口安全检测、数据防泄漏检测、数据溯源检测、数据访问行为日志合规性检测等提供靶站服务。

2.4 产品功能

2.4.1 敏感数据识别

工具内置 70+种敏感数据识别算法（例如：身份证、银行卡、中文地址等），灵活支持正则表达式、数据特征字典等算法配置功能，更好的帮助我们发现敏感数据。工具调用敏感数据识别算法，对数据库进行扫描分析，输出敏感数据信息及分布统计情况。可以清晰的掌握敏感数据资产，为监管数据安全建设情况提供基础支撑，定位监管的数据内容。

2.4.2 数据分类分级情况查验

检测企业已分类分级的数据清单中，存在的数据错分、漏分情况，根据检测结果输出分类分级准确率和召回率。通过准确率衡量被检测数据的分类分级准确性情况；通过召回率衡量企业所有数据的分类分级准确性情况。

2.4.3 数据加密合规性检测

检测企业针对敏感数据存储加密的合规性，支持检测多种加密算法加密的数据，检测数据加密的覆盖率。

2.4.4 个人信息去标识化合规性检测

适用于测试、开发、运维、数据展示等各种场景的个人信息存储去标识化检测，检测个人信息中直接标识符和准标识符的去标识化情况。支持技术扫描的方式检测数据库、日志文件；支持结合人工录入的方式检测网站&APP。

2.4.5 数据操作日志合规性检测

结合模拟工具，模拟数据访问，通过上传离线日志文件、或者连接数据库的方式，检测操作日志的合规性。检测维度包含：日志记录的全面性、准确性、完整性、日志存储时长、账号违规行为等。

2.4.6 数据库账号安全检测

检测数据库账号的特权账号、密码过期账号、锁定账号、密码即将过期账号、弱口令情况等。梳理账号的角色权限，发现异常权限配置行为。

2.4.7 数据溯源检测

可以通过模拟泄露靶站数据的行为，让企业反馈溯源结果，检查企业是否具备数据行为溯源能力或者水印溯源能力。

2.4.8 数据防泄漏能力的检测

检测企业终端设备、服务器设备的数据防泄漏能力。通过模拟多种网络协议（HTTP、FTP、SFTP 等）、终端传输渠道（蓝牙、USB 等）拨测敏感数据文件（OFFICE、

图片、PDF 等）的方式评估企业数据防泄漏能力。

2.4.9 接口安全检测

通过模拟拨测接口访问、传输敏感数据的方式，发现企业接口管控能力是否具备接口识别、接口鉴权、发现接口敏感数据明文传输、违规访问风险等。

2.5 产品优势

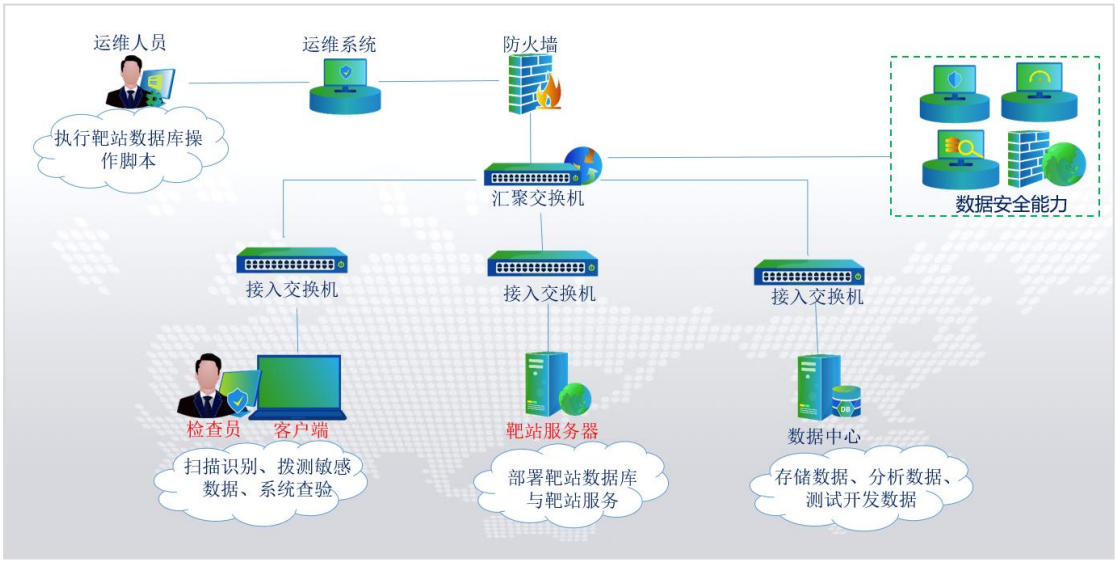
数达安全数据安全合规评估系统，实现了对数据操作日志、数据安全漏洞、数据分类分级、账号安全、敏感数据加密、个人信息去标识化等方面的合规性进行自动化监测和扫描分析，进一步输出不合规情况报表和整改建议。数据安全合规评估系统的优势及特性如下所示：

1. 部署简单：解压安装包，启动即可。
2. 便捷灵活：支持安装在 windows10 系统的笔记本上，方便携带。
3. 连接方式简单：支持在线检测，支持离线检测。
4. 丰富的报表：每项检测功能提供检测概要以及详情。
5. 支持检测不小于 5 种算法加密的数据。
6. 支持多种加密方式的检测（TDE、第三方加密系统等）。
7. 支持检测使用密码、屏蔽、抑制、假名化、置换等去标识化技术去标识化的数据。
8. 事件模型配置维度支持 20+个（sql 语句、列名、操作类型等）。
9. 支持 100+种敏感数据识别算法。

2.6 产品价值

1. 有效支撑工信部考核要求，提供行业数据模型、分级分类规则库及行业合规规则库。满足业务需要、合规需要及持续性检测需要。
2. 熟悉数据安全合规要求，了解数据安全合规动向，配套数据安全合规评估自查服务。通过合规评估平台，实现检查的规范性、效率性、可控性、可操作性，实现合规检查过程可控、结果可控、处置可控。
3. 支撑数据安全合规性检查要求同时，加强企业全方位问题发现能力，提高企业持续性合规检测灵活性。

2.7 典型部署



客户端工具检查部署图

产品支持旁路部署于用户核心交换机处，该种部署方式不需要对网络进行改动，不会对原有业务有影响。

2.8 产品规格

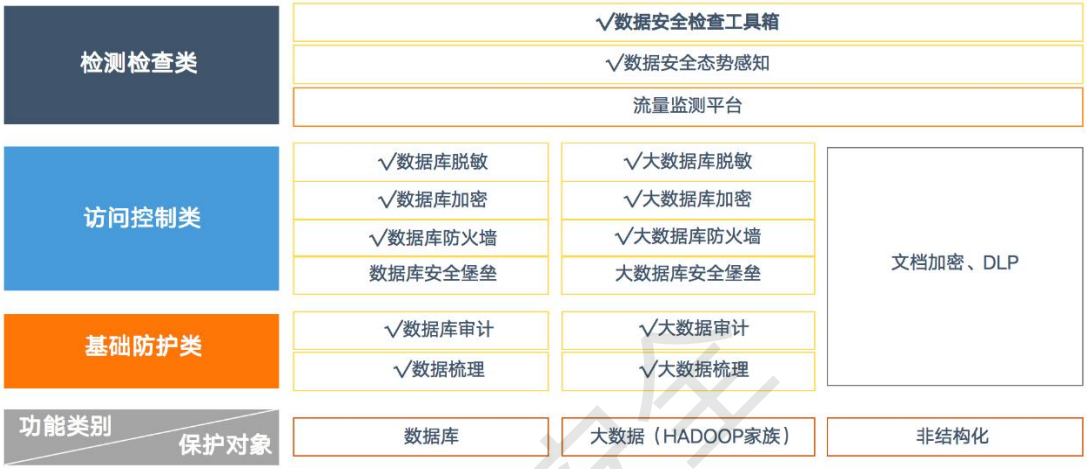
序号	产品型号	硬件配置	
1	SD-DPT-1000	CPU：六核十二线程； 内存：32G 内存； 磁盘：256G 固态硬盘+2T 机械硬盘；	数据库扫描性能 10TB/小时；

3 公司简介

重庆数达信息安全技术有限公司是数据安全领域的引领者，核心团队专注数据安全 20 余年。公司的主要目标是对数据库、大数据、文件等数据对象的存管用（存储、管理、使用）全生命周期全场景实现全面的安全防护。

公司成熟产品根据防护能力分为基础防护类、访问控制类以及检查监测和溯源类。公司还将持续推出具有高度 AI 特性的数据安全新产品。得益于深厚的技术积累，公司系列产品的功能和性能在业内处于领先。

产品矩阵如下图所示。



重庆数达信息安全技术有限公司在全国二十多个省设置了办事处，服务全国客户。