数达安全

政府行业数据安全解决方案

重庆数达信息安全技术有限公司

2023 年 5 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

摘要

为解决政府各部门中存在的数据“孤岛”问题，实现“让数据多跑路，人少跑路”的办事模式，发展智慧城市、政务云、政务大数据成为关键。其中，政务云和政务大数据平台由于所管理的数据内容敏感、使用面广、使用频率高等原因需要尤其关注其数据的安全性。传统的网络安全能力由于距离真实数据较远，无法从源头上防止数据库泄密风险。本方案以数据为中心，针对性的部署“术业有专攻”的数据安全能力体系，从数据源头解决数据安全问题。

1 需求分析

1.1 合规需求和“有用性”需求

数据泄露事件造成的影响重大，数据安全问题已经升至国家层面，有关数据安全的政策已经并正在密集出台。为了充分保障政府部门的数据安全，大数据平台和政务云需要符合国家相关的安全法律法规、技术标准和行业规范等要求，例如《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》、《GB/T 22239-2019 等保 2.0》等合规需求实现访问控制、安全审计、监测预警等能力。

在使用大数据平台和政务云相关服务过程中，需要满足用户的“有用性”需求，即数据安全能力体系确实可以发挥作用，可以有效识别并防止数据安全事件的产生。对于内部人员需要加强权限管控，防止有意无意的泄密；对于外部人员需要加强访问控制，防御外部的攻击。通过各项安全技术措施，保障大数据平台和政务云数据的可用性、完整性和机密性。

1.2 全生命周期场景需求

需要以数据为核心，构建覆盖数据全生命周期所有场景的安全保障体系。应该在数据采集、数据传输、数据存储、数据共享与使用等环节采取相应的安全防护措施保障政务云、大数据平台的数据安全。

需求	需求内容
数据采集安全	1）需要对数据采集设备进行安全管控，检查数据采集设备的安全管理措施和策略是否完善。 2）需要有完善的数据采集日志记录。 3）数据采集设备需要有完善的安全防护手段，例如身份鉴别和访问控制等。
数据传输安全	1）需要在传输重要核心数据数据时设置对应的安全措施，制定安全策略，进行安全监控。

	2）需要接口鉴权和认证能力保障数据传输的安全和被监控被记录。
数据存储安全	1）需要对数据库账号设置相应的访问权限。 2）对于重要程度很高的数据，使用加密存储，保证关键数据的保密性。 3）需要建立完善的数据备份制度，落实备份机制，保证备份数据的有效性和可用性。
数据使用安全	1）需要对使用数据使用者身份进行鉴别，防止假冒合法人员使用数据。 2）需要对使用数据的人员进行权限控制，防止数据使用者越权访问数据。 3）需要对内部人员通过应用访问敏感数据的行为进行监控和审计，并对用户行为进行建模分析，以及时发现数据滥用、泄露的风险。 4）需要对研发人员、测试人员和数据库管理员访问的数据进行脱敏，并保证数据脱敏后可用。
数据共享交换安全	1）数据资源在共享开放过程中，需要针对个人隐私信息等高敏感数据（姓名、地址、身份证号码等）进行匿名化处理，防止数据泄漏。 2）需要针对数据共享的接口进行发现、监控和审计，防止数据泄露。 3）如共享的数据不慎泄露，需要进行溯源追责。
数据销毁安全	1）需要有效的数据销毁手段。 2）需要建立数据销毁工作记录和资源回收清单。 3）需要完善的数据销毁安全管理制度，覆盖全部的销毁场景。

1.3 委办局多租户需求

需要基于云安全服务平台，面向租户提供安全云服务能力，包括数据库审计服务、数据库加密、数据脱敏服务等。若在使用此类服务时，未保证租户权限在管辖范围内且未限制对数据的操作权限，则有可能出现权限管理混乱的情况。当租户误操作属于自身以外的数据，导致数据丢失或泄露等问题时，将对数据安全造成极大影响。

1.4 安全服务及持续加固需求

由于内部人员可能存在数据安全知识匮乏或者专业性不够等问题，所以需要专业的数据安全服务，协助用户进行数据安全运营、数据风险评估等，保障数据在使用过程中的安全。

数据安全是一个动态变化的过程，需要持续对业务系统进行加固，根据变化做出调整以应对新的风险。基于此方面考虑，需要周期性的数据备份、数据安全能力的增设、安全设备和策略的更新、安全评估和漏洞修补。

2 解决方案

2.1 合规需求和“有用性”解决方案

为满足网络安全法、数据安全法、等级保护、国密要求、隐私保护、内部标准等，数达安全解决方案参照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》、《GB/T 22239-2019 等保 2.0》等法律法规，在深入研究、全力落实好国家及省相关政策基础上，紧密结合实际情况，进一步研究制定具体的、有针对性的政策措施，如：数据分类分级、数据加密、访问控制、安全审计、风险告警等。利用安全产品组合部署，通过及时监测和预警，实现动态联防，帮助最大限度达到合规要求。

针对用户的“有用性”需求，数达安全提供的产品可以实现身份鉴别、访问控制、安全审计、数据加密等对数据的保护措施。可针对内部人员和外部人员分别定制管控措施，有效防止数据安全事件的发生。同时对所有数据操作记录和溯源，有效保障大数据平台和政务云数据的可用性、完整性和机密性。

2.2 数据全生命周期安全解决方案

以数据资产梳理与数据流转监测为基础，通过对数据大数据平台或者政务云的数据进行分级分类安全梳理，结合访问控制、数据加密、数据脱敏技术对不同用户角色、不同的数据访问行为进行管控、防护、脱敏、审计、分析，基于“可视、可管、可控”的思路，建设一套提醒化的数据安全平台，实现数据全生命周期的数据安全。同时通过对所有数据安全产品的日志收集和分析，系统展示整体数字资产情况，敏感数据分布、流向状态，以及数据泄露中的追踪溯源问题。

需求	解决方案
数据采集安全	部署数据库加密、运维脱敏、数据库防火墙、数据审计等安全能力，实现完善的安全管控策略，生成采集时日志、实现完善的安全防护手段，如双因子认证、访问控制等。
数据传输安全	1）通过数据库防火墙对重要核心数据设置对应的安全措施，制定安全策略，进行安全监控。 2）部署数据接口安全系统，与数据库防火墙系统、数据库审计系统联动保障数据传输的安全和被监控被记录。
数据存储安全	1）通过数据库加密对数据库账号设置相应的访问权限。 2）通过数据库加密对重要程度很高的数据进行加密存储，保证关键数据的保密性。 3）部署数据备份机制，保证备份数据的有效性和可用性。
数据使用安全	1）数据库防火墙可对使用数据使用者身份进行鉴别，防止假冒合法人员使用数据。

	2）数据库加密系统可对使用数据的人员进行权限控制，防止数据使用者越权访问数据。 3）通过数据库审计系统对内部人员通过应用访问敏感数据的行为进行监控和审计，并对用户行为进行建模分析，以及时发现数据滥用、泄露的风险。 4）通过数据库脱敏系统对研发人员、测试人员和数据库管理员访问的数据进行脱敏，可根据需求进行静态或动态脱敏，满足数据的可用性。
数据共享交换安全	1）通过数据库脱敏系统，针对隐私信息等高敏感数据进行脱敏处理，防止数据泄漏。 2）API 审计系统可以针对数据共享的接口进行发现、监控和审计，防止数据泄露。 3）数据库静态脱敏可以在脱敏过程中对数据添加水印，方便数据泄露后的溯源追责。
数据销毁安全	1）部署数据销售设备，实现数据的安全销毁。 2）通过数据安全态感，实施监控数据流和数据存储，确保已经销毁的数据不再出现。

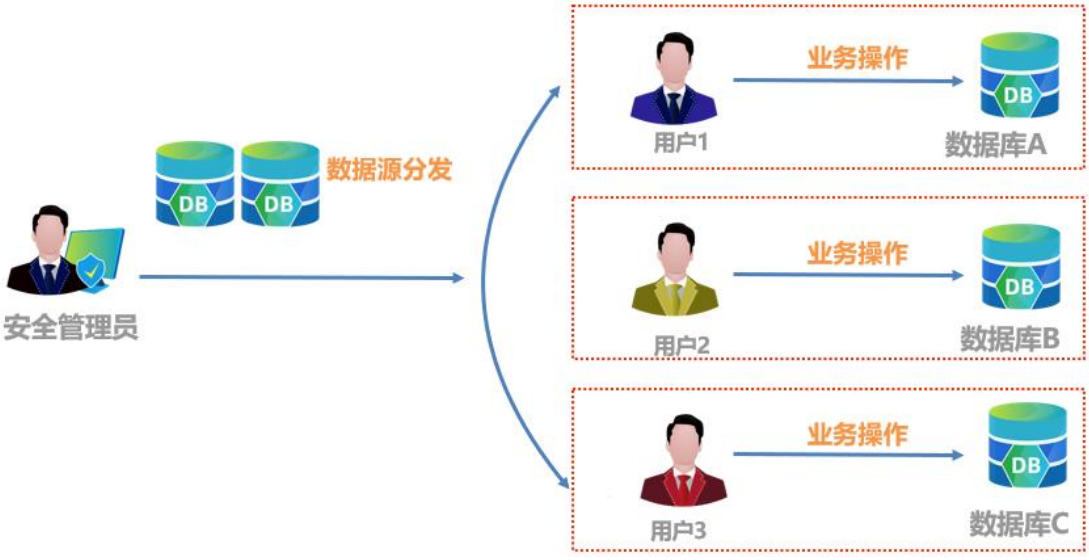
2.3 委办局多租户解决方案

严格落实《网络安全法》、《数据安全法》规定和网络安全等级保护基本要求，按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，明确委办局对数据局的数据安全主体责任，实现多租户管理。

对于使用云安全能力租户的系统和工作人员：

（1）云上的租户可以选择是否用数据库审计、数据库防火墙、数据库加密和数据脱敏等，此时数安能力以虚拟机实例，或者多租户的方式部署；

（2）租户的运维人员通过安全运维访问数据库，只管理自身部门的数据，并可以防止云上租户内部办公人员通过截屏等方式泄漏敏感信息。



2.4 安全服务及持续加固解决方案

在深入研究、全力落实好国家及省相关政策基础上，紧密结合实际情况，进一步研究制定具体的、有针对性的数据安全服务。围绕政务云和政务大数据平台的建设和定位，展开有用的数据安全服务内容：

服务项	服务内容
数据安全运营服务	建立常态化数据安全运营体系机制，包括风险预警、巡检自查、应急响应、问题处置、安全策略优化、数据使用状况的监控等。
数据风险评估服务	通过对各类数据进行综合分析，最终确定数据资产存在的问题，并在此基础上确定数据风险的级别。
安全咨询规划服务	基于数据安全建设实践、国内外数据安全发展趋势研究及国家相关政策要求形成的数据安全评估服务，以安全环境、主机安全、应用安全、数据库安全、中间件安全进行综合评估，分析安全功能设计及存在的安全隐患、是否符合应用运行安全需求，并针对问题提供解决方案建议。

数据安全威胁不断变化，数据安全价值不断增大，所以数据安全需要持续加固，以应对不断变化的安全威胁和技术风险：

服务项	服务内容
定期备份数据	定期备份数据并建立灾备机制，以便在紧急情况下能够快速恢复数据，并避免数据的永久损失。
安全设备配置和更新	定期巡检部署的安全设备，如数据库防火墙、数据库审计，数据库加密等，保证其正确运行，并在新版本发布后及时通知用户进行升级。
跟踪和升级安全措施	从风险评估、攻击趋势、技术演化等角度跟踪安全威胁和漏洞，并随时根据最新情况和变化对安全措施进行完善和升级。

3 产品能力

3.1 数据资产安全管理能力

数据资产安全梳理可为用户提供全域数据资产智能挖掘和扫描梳理，依据用户对数据资产的价值、敏感度、类别等具体界定，进行数据分类分级的标示、敏感数据扩散边界控制、风险动态监测和防护等。同时利用数据安全智能识别引擎及可视化技术直观呈现数据分布、状态、流转、关联等详细信息。

3.2 数据加密能力

由数据库加密系统实现数据加密能力，基于透明加密技术实现敏感数据加密存储。支持多种加密算法对敏感数据加密，以满足等保、分保等评测要求；在此基础上增加独立于数据库的访问授权机制。任何访问被加密数据的人或应用事先

必须经过授权，拥有合法的访问权限才能访问加密数据，非授权用户无法访问加密数据，有效防止管理员越权访问及黑客拖库。

3.3 数据脱敏能力

拥有数据库脱敏静态脱敏和动态脱敏两种模式，支持替换、截断、屏蔽、随机、加密、隐藏等脱敏算法和策略，支持删除、编辑等高危操作禁止，限制返回行数等动态访问控制策略。能够解决大多数用户针对合规性满足以及敏感数据泄露防护等场景的业务需求。

3.3.1 数据库动态脱敏

数据库动态脱敏支持屏蔽、随机、仿真等类型的脱敏算法，基于数据分级分类标准和用户访问数据的权限，在生产数据库的数据传输和展现过程中，对数据进行实时的模糊化处理，防止敏感数据的泄露，满足运维场景中的实时数据脱敏的需求。

3.3.2 数据库静态脱敏

通过特定算法规则对敏感信息进行变形和隐藏，批量的将敏感数据转换为非敏感数据。脱敏后的数据特征看上去和原有数据一致。在实施高效脱敏的处理的同时，提供脱敏后数据的高保真性、数据之间的关联性，支持脱敏工程的可逆性和不可逆性、可重复性与不可重复性的多种策略选择。充分满足用户针对不同应用场景下的各种脱敏需求，使脱敏后的数据可以安全的应用于测试、开发、分析和第三方大数据分析等环境。

3.4 数据访问控制能力

其主要功能包括独立访问控制、SQL 注入攻击防护、漏洞攻击防护、风险检测与处置以及全面日志审计等。

（1）独立访问控制：数据库防火墙通过接管数据库访问，并针对 SQL 协议进行解析，实现独立于数据库权限体系之外的访问控制功能。支持添加内置和自定义访问控制规则、支持经典的黑白名单以及基于机器学习的智能动态基线机制。

（2）SQL 注入攻击防御：数据库防火墙通过分析 SQL 语法来识别 SQL 注入攻击的不同特征，同时构建 SQL 注入特征库，对外来 SQL 注入攻击进行特征库匹配。同时基于信息独有的 SQL 序列智能检测发明专利，快速有效的对 SQL 注入攻击进行拦截阻断。

（3）虚拟补丁：基于传统数据库补丁升级带来的业务影响，数据库防火墙有针对性的开发虚拟补丁功能。通过内置缓冲区溢出、拒绝服务等多种数据库虚

拟补丁规则，涵盖数十种数据库类型，在数据库外层构建漏洞攻击的专项防护，有效规避数据库被攻击的风险。

（4）风险告警：数据库防火墙对识别的风险访问行为记录形成风险告警日志，外发并进行阻断。告警信息根据匹配的策略进行分类后统计汇总。对于系统产生的误报警，可以分别进行处理，提高防护策略的精确性。

3.5 数据安全审计能力

3.5.1 数据库审计

数据库审计用于实现对数据访问的所有行为的记录，支持旁路审计、代理审计和插件审计三种工作模式，通过对数据流量进行深度解析来实现对数据库访问行为的审计，帮助用户实时统计访问数据库的请求和风险，提升数据库运行监控的透明度，降低人工审计成本，真正实现数据库全业务运行可视化、日常操作可监控、危险操作可控制、所有行为可审计、安全事件可追溯。

数据安全审计系统还提供灵活的告警策略、细粒度的审计日志和合规性的报表，解决客户的核心数据库面临的“越权使用、权限滥用、权限盗用”等安全威胁，满足各类法令法规对数据安全审计的要求。

3.5.2 API 审计与溯源

API 业务审计系统以旁路部署侦听的工作模式，能对 Web 业务系统的接口进行深度解析与审计分析，可以帮助用户提升业务运行监控的透明度，降低人工审计成本，真正实现业务全业务运行可视化、日常操作可监控、危险操作可控制、所有行为可审计、安全事件可追溯。

API 业务审计系统还提供灵活的告警策略、细粒度的审计日志和合规性的报表，解决客户的核心业务面临的“敏感信息外发、接口盗用、违规权限、业务风险”等安全威胁，满足各类法令法规对业务接口审计的要求。

3.6 数据防泄漏能力

数据防泄漏基于先进的 AI 识别算法，通过对文档自动分类分级，实现数据有效治理；以深度内容分析为基础，对企业内部外泄内容进行识别，发现敏感数据的传输与应用；结合文件加密技术，保护重要数据资产安全，有效防止核心数据主动、被动泄密。为用户提供安全、高效、稳定、易用的一体化数据安全整体解决方案，有效防止数据泄漏事件发生。

3.6.1 终端防泄漏

终端 DLP 主要用于安装在员工笔记本或台式机上，负责扫面发现这些终端

上敏感数据，并监视这些终端上敏感数据的操作使用，对于高风险数据的复制、USB 拷贝、打印刻录等行为进行风险提醒和阻断保护。

3.6.2 网络防泄漏

网络防泄漏系统部署在组织网络中，通过流量牵引技术，对受控区域内的外发流量进行深度解析、内容恢复和敏感度扫描，及时发现受控区域内通过网络泄漏数据、传播数据的行为，并进行拦截、告警、审计等措施，能够根据网络环境和监控需求，进行灵活多变的部署。系统支持通过旁路、串联、代理、对接等模式，对从网络中获取流量进行协议识别、内容恢复与扫描，及时外发、下载的电子邮件，上传、下载到各种 Web 应用或文件服务器数据终是否包含有敏感数据，并对违规流量进行实时告警、拦截等处置。

3.7 数据安全态势感知

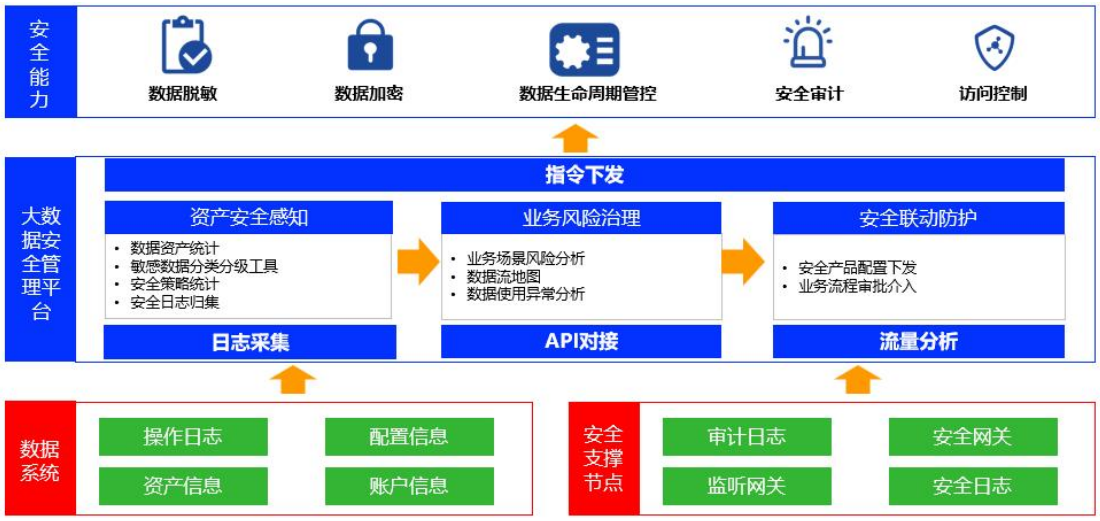
数据安全态势感知系统实现了数据安全能力的融合和一站式统一管理。用于集中管理数据安全系列组件，实现统一认证、账户审计、授权管理、设备管理、状态检测等功能，实现安全组件的实时状况监控、报警/报表信息的集中展现。实现“一窗式”运维管理、设备的快速定位，以及高安全冗余备用方案。同时通过人工智能手段，实现对数据的 APT 攻击等复杂攻击行为的识别。为机构 IT 主管、信息部门领导提供及时、全面、准确的全网数据安全管理的量化分析和决策依据，同时有效提升管理员日常运维、管理效率。

部署在用户环境中的所有安全组件可以通过数据安全态势感知系统进行统一管控。系统能够提供全网数据安全产品的实时监控，包括设备运行的状态、性能，能够通过平台进行统一的维护管理，例如策略配置，资产监控和常见维护操作。同时，管控平台能够进行报警通知，生成安全报表等。

4 案例分享

4.1 某市智慧城市项目

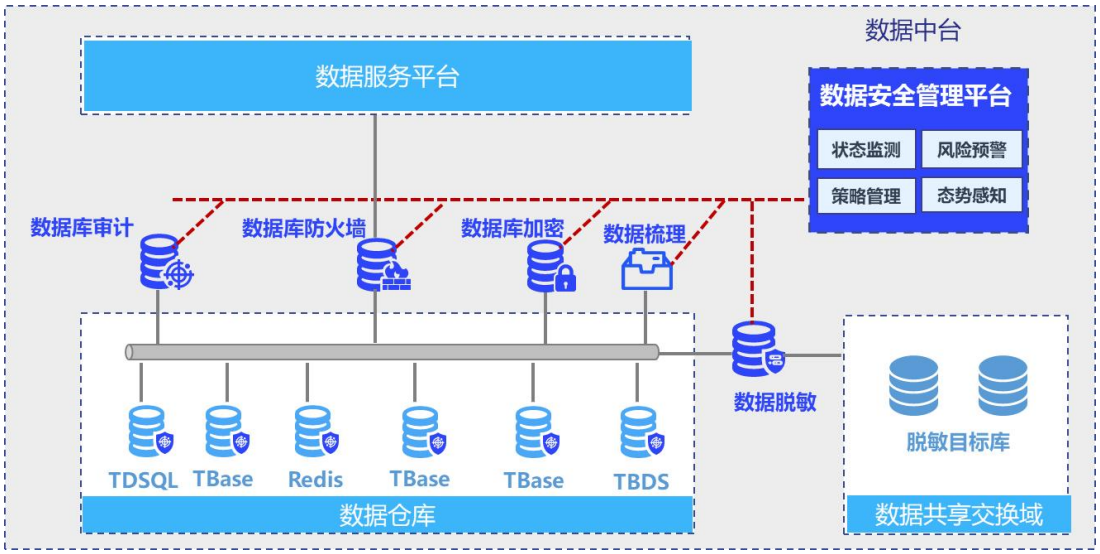
某市智慧城市在数据安全风险、租户与云服务商责任难以界定、客户对数据和业务系统的控制能力减弱等问题，在法律法规、安全功能、自身业务保障上都存在需求。因此，需要采用适合实际环境的数据安全全生命周期解决方案和服务，从各维度考虑安全方法和体系、联动防护的机制、安全策略的管理，保障大数据安全和云租户安全。以等保为基线构建主动、可信的云安全防御体系，实现 “数据大脑”安全系统的统一协同运营，保障 “数据大脑”的网络空间安全、稳定，智慧系统持续、有序、安全运行。



4.2 某省大数据中心解决方案

根据该省大数据发展管理局要求，发现在现有体系下存在多方面的数据安全风险。例如数据明文传输导致数据泄露风险、数据明文存储导致的数据泄露风险、安全运维人员权限过高导致的数据泄露风险、能力开放平台数据共享交换场景中的数据泄露风险。同时该省对于数据全生命周期的保护机制提出要求。

在实际部署中，以数据资产梳理与数据流转监测为基础，通过对数据中台的数据进行分级分类安全梳理，结合访问控制、数据加密、数据脱敏技术对不同用户角色、不同的数据访问行为进行管控、防护、脱敏、审计、分析，基于“可视、可管、可控”的思路，建设一套体系化的数据安全平台，实现数据全生命周期的数据安全。同时通过对所有数据安全产品的日志收集和分析，系统的展示整体数字资产情况，感知敏感数据流向状态，解决数据泄露中的追踪溯源问题。



5 数达安全简介

重庆数达信息安全技术有限公司（以下简称数达安全），成立于 2021 年 6 月，总部位于重庆，分设重庆研发中心和北京研发中心，以及上海分部、南京分部和深圳分部，销售团队覆盖西南、西北、华东、华北等全国省市区域。

数达安全专注数据安全领域，核心团队专注数据安全已经 20 余年。公司成熟产品根据防护能力分为检查监测和溯源类、访问控制类、基础防护类，产品范围涉及数据库、大数据、文件等数据对象的存管用（存储、管理、使用）等，已广泛应用于电信运营商、政府、科研、军工、公安、教育、能源、企业、医疗等行业，与多家知名网络安全企业达成战略合作。

数达安全以“用核心技术，守护数据价值与安全”为使命，立足创新与发展，致力于为客户提供高性能、高稳定的产品和服务，为促进数字经济健康发展贡献力量。