数达安全

面向业务专网的数据安全解决方案

重庆数达信息安全技术有限公司

2023 年 8 月

目录

1 前言

由于各企事业单位业务专网的特殊性，涉及的数据敏感，且数量大、范围广，所以数据安全成为一个备受关注的问题。。但是，由于长期以来的信息安全偏重于网络安全和文件安全，对结构化数据的安全防护有所不足。本方案数据为中心，针对性地建设“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。

2 需求分析

2.1 合规性需求及有效性需求

某用户应用系统中承载大量重要且敏感数据信息，然而这部分敏感数据信息在传输过程、存储过程都是以明文形式，且系统的登录方式依然是最基础的用户名和密码登录。整体来看，缺乏针对应用和数据的安全保护手段，在现阶段不满足上级主管单位对数据保护的要求。在数据保护方案中，用户有从运行管理、身份鉴别、访问控制、安全审计、存储加密和数据库安全方面进行一系列技术防护和测评的需求。

在用户业务系统满足合规之后，还要确保数据安全体系的有效性。即在各种数安能力的保护下，保障数据全生命周期的安全，保障数据的可用性、完整性和机密性。

2.2 防攻击需求

现阶段，对真正处于核心层的敏感数据载体－数据库的保障能力较低，同时针对数据的攻击越来越组织化、体系化，抗攻击能力严重不足，成为数据安全防护的“短板”。

2.3 加密保护需求

用户业务专网信息系统要求对内高度保密，要求对包括生产、检验等内部人员高度保密，而设计图纸的敏感性和重要程度则更不言而喻，这要求用户对此类敏感信息必须运用加密技术进行存储加密保护。

2.4 外发保护需求

业务专网信息系统内产生的数据和文档有高度保密性、高度敏感性，数据泄露会造成严重后果。且移动设备如笔记本电脑、U 盘使用广泛，与外部单位的合作时，存在对外发送文件数量较多的情况，容易造成大量的数据泄露事件。

2.5 传输溯源需求

业务专网信息系统内的各业务系统之间数据交互频繁，敏感数据和文件在内部访问传输行为需要可追溯。

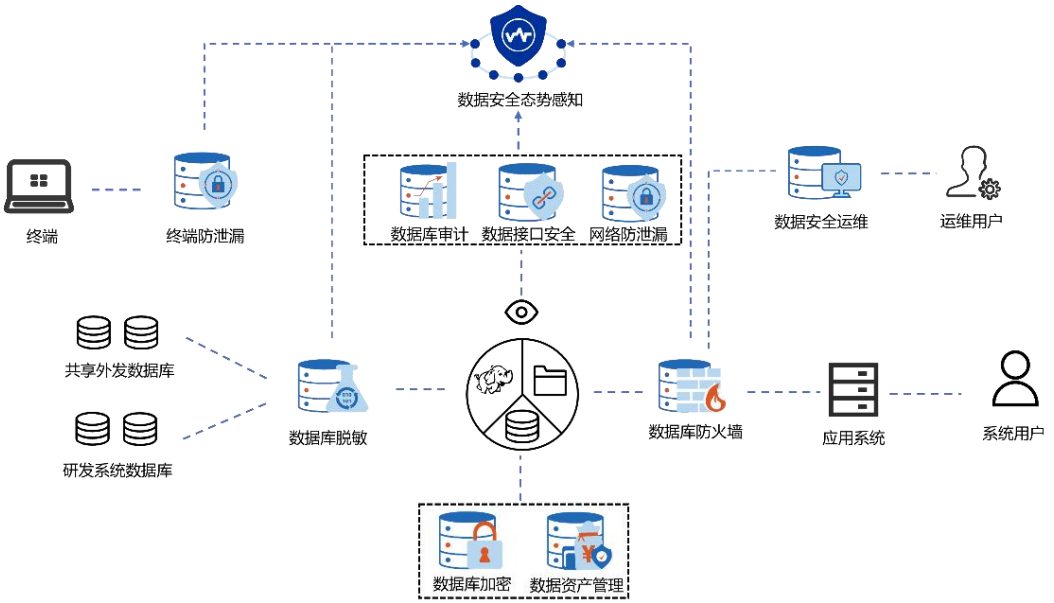
与合作单位有大量的对外接口，这要求用户必须加强对接口的管理以及接口中敏感数据的传输管理。且对外发送的数据需要添加水印，方便数据泄露后的溯源定责。

3 技术方案

3.1 合规性需求和有效性解决方案

为满足网络安全法、数据安全法、国密要求和各行业标准，数达安全面向业务专网敏感数据的安全解决方案参照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等法律法规，在深入研究、全力落实好相关政策基础上，紧密结合实际情况，进一步研究制定具体地、有针对性的政策措施。比如：数据分类分级、数据加密、访问控制、安全审计、数据防泄漏、接口安全、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。

针对用户的有效性需求，本方案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、数据防泄漏、接口安全等对数据的保护措施。可针对不同权限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，有效保障敏感数据的可用性、完整性和机密性。具体能力部署情况如下图所示：



数据资产管理系统可以将数据分类分级并打标，梳理后可提供给其他数安能

力进行防护策略的定制；数据库防火墙实现数边界的隔离，进行访问行为控制，抵御针对数据库的攻击；数据库安全运维提供安全运维平台，防止 DBA 账号泄露和提权攻击的风险，接入防火墙加强访问控制；通过数据库加密实现表空间和字段级的加密；终端防泄漏安装在终端电脑上，防止内部文件非法向外传输；通过数据库审计、数据接口安全、网络防泄漏对访问流量进行监控和分析，对违规结构化数据、非结构化数据和接口的访问行为进行实时告警；使用数据库脱敏系统将敏感数据脱敏，并用于研发、测试、对外发送等场景；数据安全态势感知通过收集所有数安能力的日志进行联动分析和全面的风险预测。

3.2 防攻击解决方案

针对用户业务专网系统抗攻击能力的不足，通过部署数据库防火墙系统、数据库审计系统和数据库安全运维管理系统进行联动，增加数据库的安全性。

数据库审计系统能够实时监控记录用户对数据库的所有访问行为，并对数据库所遭受的风险行为进行告警，帮助用户快速生成事后合规性报表，同时对事故追根溯源。通过全面监控内、外部数据库的访问行为，分析出其中的攻击行为，生成策略下发到数据库防火墙中。

数据库防火墙系统通过全面的数据库通讯协议解析，基于身份鉴别和行为分析的主动防御机制，能够主动实时监控、识别、告警、阻断针对数据库的安全威胁，实现用户的行为特征分析、访问行为监控和危险操作阻断。

数据库安全运维管理系统进一步对运维人员的权限进行进一步细化，对于授权用户，可以查看相关敏感数据，对于非授权用户则通过屏蔽敏感字段、截取敏感字段等多种方式确保敏感信息不被泄露。在满足系统运维的前提下保障用户数据安全。

3.3 加密保护解决方案

对于结构化数据，例如敏感信息数据库的保密，通过数据库透明加密系统实现。系统基于加密算法和合理的密钥管理，实现字段级和表空间级的加密。同时通过独特的解密权限控制技术，使得用户只能够读取已被授权访问的加密表和字段。通过数据库透明加密系统可以做到对存储介质泄密和 DBA 权限泄露导致的泄密的规避。

对于非结构化数据，例如设计图纸和文件等，则通过终端防泄漏系统进行保护。系统融合机器学习、关联分析、密码技术、访问控制、数据标识等多种技术以数据为中心，分类分级为基础，为用户数据资产提供事前主动防御、事中实时

监测、事后追踪溯源、全程态势感知，基于数据的全生命周期提供全方位、立体化防护。

3.4 外发保护解决方案

对于敏感数据，可以通过数据库脱敏系统对敏感数据脱敏，在保证数据可用性的前提下去除敏感信息，从源头上防止数据库泄露的发生。同时部署网络防泄漏系统，对受控区域内的外发流量进行监控，识别邮件、文件等敏感数据，进行实时告警和拦截。

3.5 传输溯源解决方案

对于合作单位的对外接口，通过部署接口安全管理，可以实现高效率的自动化数据接口识别；提供统一标准的数据对外合作报备和审批方案；能够依据数据对外合作备案结果对接口使用情况进行评估。同时数据接口安全管理还提供数据接口审计功能，保障数据安全合规的同时增强全方位安全侦测能力。

用户业务专网系统内的信息交换和外发数据都可通过静态脱敏系统添加水印，方便追溯数据源和数据泄露追责。

3.6 安全服务

在深入研究、全力落实好国家及行业相关政策基础上，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。围绕用户业务专网的建设和定位，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，分析数据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。

4 产品能力

本方案针对用户业务专网提供完整的数据安全建设体系，通过各种数安能力保护结构化数据、非结构化数据和大数据系统。

4.1 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识、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。

4.2 数据库加密能力

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，以满足主管单位的行业评测要求；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。

本产品实现了两个主要目标：

1）规避存储介质泄密风险

敏感数据以密文的形式存储，这样能保证即使在存储介质被窃取，或数据文件被非法复制的情况下，敏感数据仍是安全的。

2）规避提权攻击导致的泄密风险

通过密码技术实现三权分离，必须同时得到 DBA 授权和加密系统授权才可以访问加密数据，实现了对特权账号的分权管理，从而避免 DBA 权限泄漏带来的批量数据泄漏风险。

4.3 数据库静态脱敏能力

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、分析和第三方数据分析等环境。

4.4 数据库安全运维能力

数据库安全运维为 B/S 架构设计，采用典型的应用部署方式，客户端无需安装任何程序，每个用户都以个人身份操作数据库，无需记住数据库复杂、众多的各类密码。数据库安全运维是一款具有跨平台、低成本和高度安全性的数据库运维产品。

数据库安全运维提供统一的组织管理方式，能够批量的管理各类运维账号。同时针对每个运维账号的使用人员，采用多种组合的认证方式，包括多因子、合

规审查等鉴别手段，能够唯一认证用户身份，并监控运维账户的每一个操作和SQL 的执行，极大的简化了运维账号的管理成本。

数据库安全运维具有全方位、多层级的权限管理体系，能够精细化的控制运维账号的权限。数据库安全运维提供的权限控制级别包括：库级、模式级、表和数据对象级、列级、行级、数据级。通过全方位的授权控制，能够将运维账号的权限固定在业务需要的最小范围内，有效的杜绝了数据库运维账号的权限滥用、越权访问等安全隐患。

数据库安全运维内置了丰富的敏感数据识别规则，能够自动发现数据库中存在的各类敏感数据，针对敏感数据访问提供了多种脱敏规则可选，最大化的减少了敏感数据的暴露面，防止数据在运维环节被越权访问和非法窃取，提升了隐私数据在各个环节的安全性。

4.5 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：考虑到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。

4.6 数据安全审计能力

数据库审计用于实现对数据访问的所有行为的记录，支持旁路审计和插件审计两种工作模式。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。

4.7 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。

4.7.1 终端防泄漏能力

终端防泄漏能力主要用于安装在用户的笔记本或台式机上，负责扫描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。

4.7.2 网络防泄漏能力

网络防泄漏能力部署在组织网络中，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。

4.8 数据接口安全能力

数据接口安全能力对流量采集、重组、数据包过滤持久化存储和索引与安全分析实现对邮件、http(s)、samba、ftp(s)等数据传输协议的监控，从而实现对外部网络攻击流量分析、内部风险监测对外开放共享风险监测。支持多种接口类型识别、支持对外开放规则定义、可预警安全事件及敏感数据。主要解决的问题为：

（1）缺少数据综合监测手段：现有流量监测方式单一，缺少数据库（传统）、大数据、非结构化监测手段。

（2）缺少对外开放共享监测手段：对外开放共享接口数量繁多，缺乏统一管理手段，接口传输敏感数据难发现。

（3）缺少接口敏感信息监测手段：缺少对接口中敏感数据传输情况的监测能力。 无法透视、监测传输内容。

（4）安全链上下游结合：缺少跨平台结合能力，无法与安全链上游（如态感），下游（数据安全防护能力）有效整合。

4.9 数据安全态势感知

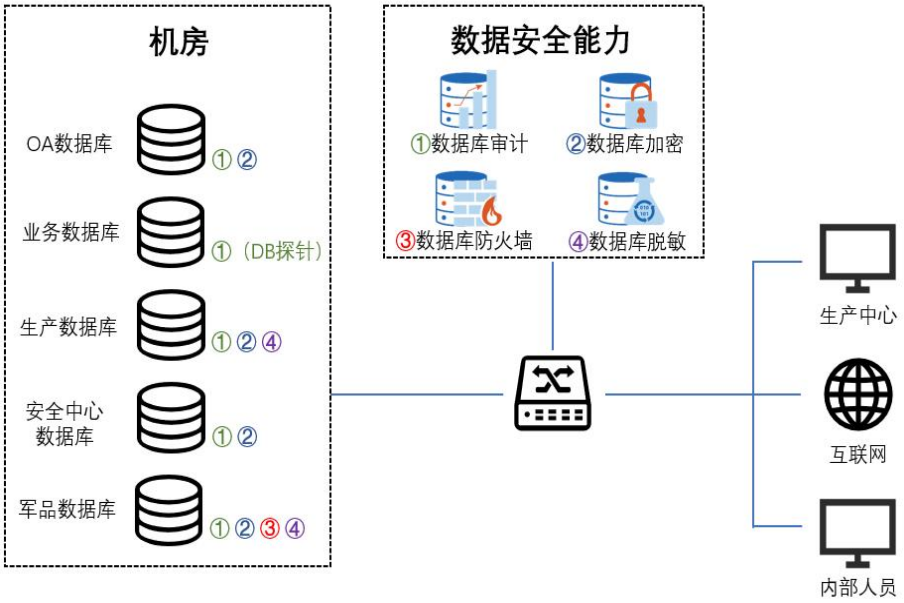
数据安全态势感知系统实现了数据安全能力的融合和一站式管理。用于集中管理数据安全系列组件，实现统一认证、账户审计、授权管理、设备管理、状态检测等功能，实现安全组件的实时状况监控、报警/报表信息的集中展现。实现“一窗式”运维管理、设备的快速定位，以及高安全冗余备用方案。同时通过人工智能手段，实现对数据的 APT 攻击等复杂攻击行为的识别。为机构 IT 主管、信息部门领导提供及时、全面、准确的全网数据安全管理的量化分析和决策依据，同时有效提升管理员日常运维、管理效率。

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，资产监控和常见的维护操作。同时，管控平台能够进行报警通知，生成安全报表等。

5 案例分享：某研究所

5.1.1 需求背景

某研究院其研发网络、外部访问及内部访问均处于同一环境中，内网流量复杂，且流量为非加密状态。办公数据库服务器、业务数据服务器、生产数据库服务器、安全中心数据库服务器及产品数据库服务器均通过同一核心交换机访问。同时针对不同的数据库服务器需要部署不同的数据安全保护能力。



5.1.2 业务痛点

- 访问数据库账号权限控制颗粒度不够；
- 可能遭受外网攻击；
- 生产中心人员可能泄露敏感信息。

5.1.3 解决方案

通过两期建设，实现该客户的综合数据安全管控。

第一期：通过部署数据库防火墙和数据库审计对来自外部的 SQL 注入攻击进行检测、流量进行可视化监控，保障数据安全。对生产中心人员使用的敏感数据进行脱敏，保持数据可用性的同时保证敏感数据不外泄。通过数据库加密、数据库防火墙达到对访问数据库权限的细颗粒度控制，从物理、社会学、技术层面上保障数据存储和访问的安全。

第二期：补充部署数据防泄漏、数据安全运维系统、数据安全接口管理系统、以及数据安全天眼系统，完成数据能力体系的闭环建设。

5.1.4 方案价值

- 可视化监控数据库流量及状态，对风险实时响应；
- 多维度的保护数据安全，防止敏感信息泄露；
- 针对数据库字段、行级别的细颗粒度的访问控制；
- 满足行业合规性要求，同时满足数据安全策略的有效性需求。