数达安全高校数据安全解决方案

摘要

随着教育信息化的推进，高校数据中心建设已经成为学校信息化建设的重点，它承担了数据汇集、数据管理、数据服务等任务，是对校园信息系统中的数据进行集中存储、共享和交换的核心枢纽。但随着高校网络中的数据量不断增多，数据安全问题发生的也越来越频繁，给高校网络中心的管理人员提出了巨大的难题，也给高校千万师生的信息安全造成了巨大威胁。且当前《网络安全法》《数据安全法》以及《个人信息保护法》，都相应指出了对于数据保护的相关要求和责任，强调了数据安全的重要性。

数达安全高校数据安全解决方案旨在提出切实可行的防护措施，提高高校数据安全防护能力，切实维护高校数据安全。利用“能力+管理+服务”三位一体的思路，并利用相关技术能力，实现围绕数据全生命周期的数据安全防护。目前也已为多所高校提供了切实有力的防护措施。

1 背景分析

1、事件回顾

自从进入信息化时代以来，高校数据泄露事件频频发生。高校作为数据安全的重灾区，很容易遭受来自国内外的网络攻击，别有用心者往往就盯上了高校的科研数据、学生和教师的个人隐私数据、学校的教务数据，以及网络设施数据。比如说这些近十年内在高校发生的数据安全泄露事件，如 2014 年乌云漏洞平台发现的多所学校存在网站存在 SQL 注入漏洞；2016 年，山东籍大学生徐玉玉、宋振宁，因信息泄露引发的电信诈骗，最终使得两个年轻大学生失去生命。2020 年多个高校出现学生“被就业”的情况；2022 年某校数据库信息被公开售卖，造成一亿多条数据被泄露；2022 年西北工业大学遭美国攻击上千次，泄露大量设计国家安全的敏感信息。这些事件都暴露了高校在数据安全方面存在较大漏洞。而这些事件的发生，往往造成了个人权利被侵犯，高校科研、经费、人事信息流失，甚至危害到国家安全。而且隐私数据被泄露也会影响社会公平正义，导致学生对学校不信任，不利于社会和谐的局面。师生个人隐私数据泄露，也可能造成人身财产安全遭受威胁，或被人利用非法获利，或被犯罪分子利用，从事电信诈骗，危及生命安全。

2、泄露原因分析

针对当下高校数据泄露的原因，我们做了以下几个要点进行分析。

一是内部人员违规：由于高校多数内部人员数据安全意识淡薄，可能存在无意识的疏漏，且不法分子可能会利用社会工程学从高校工作人员、第三方维护人员处获取校内隐私数据，使得内部违规或犯罪事件呈上升趋势。

二是法规政策落地迟缓：在三法一例（网络安全法、数据安全法、个人信息保护法、关键信息基础设施安全保护条例）正式实施之前，高校主要基于等级保护来作为数据安全防护的依据。但是到现在为止，高校的数据安全监督管控体系依然没有健全，导致在高校侧数安防护体系建设迟缓。

三是数据安全能力和制度建设落后：当前高校存在的情况依然是利用传统网络安全边界的防护手段，但是这些网络层面的访问控制无法判别具体的数据库访问活动，更做不到细粒度的审计，无法解决数据库层面带来的数据安全隐患问题。同时在数据安全管理制度方面，由于没有相关标准和规程，导致无明确和规范的管理制度来约束，致使相关防护不足。

四是专业人才不足且系统复杂：高校的系统环境十分复杂，且应用和数据分散，容易形成数据孤岛，导致数据安全管理十分困难；数据中心和业务处室的相关安全责任划分不明确，也形成了数据安全的三不管的现状；且在高校内相关管理人员对于数安的保护意识薄弱，专业数据安全人员又十分匮乏，很多管理人员都是由老师身兼数职，无法满足人力保障的需求。

3、现在必须重视数据安全

当前我国近年来颁布了相关的法律也明确了对于数据安全的重视程度，包括《网络安全法》《数据安全法》以及《个人信息保护法》，都相应指出了对于数据保护的相关要求和责任，强调了数据安全的重要性。同时在教育行业，针对教育系统数据的保护也相应出具了行业规范要求，明确了教育系统数据相关管理办法。如 2021 年教育部等七部委印发《关于加强教育系统数据安全工作》的通知：要求建立教育系统数据安全责任体系和数据分类分级制度，形成教育系统数据资源目录；健全覆盖数据收集、传输存储、使用处理、开放共享等全生命周期的数据安全保障制度，开展常态化的数据安全监测预警通报。这些相关法律法规的制定，从内外部结合体现了当下高校必须重视数据安全。

2 需求分析

1、高校应用和数据分布

目前高校的 IT 系统主要集中于计算中心，一般都是采取物理机和私有云的

模式部署在计算中心机房。其中系统众多，各系统管理人员分布则比较分散。校内会建成校园大数据系统，来集中所有系统的数据，但是像财务、一卡通、图书馆管理等大系统则是独立运行。

2、高校数据安全风险分析

高校系统主要面临的数据安全风险则主要包括了以下几点：一是系统内的数据没有进行分类分级达标的工作，没有检测数据发生变化的实时性检测手段；二是相关的运维或管理人员因为权限过高，可以查看存储的敏感数据，就可能造成数据泄露的风险；三是敏感数据没有进行加密存储；四是开发测试使用的数据皆为真实数据，没有进行脱敏等手段进行处理；五是没有实现数据层攻击检测手段和接入的许可控制手段；六是对数据访问和流转的过程没有采取相关留痕和事后溯源的措施；七是在校园内部缺乏对于邮件数据安全的检测能力；八是整个校园内的数据安全缺乏时间分析和整体的态势展示措施。

3、高校数据安全之特殊痛点分析

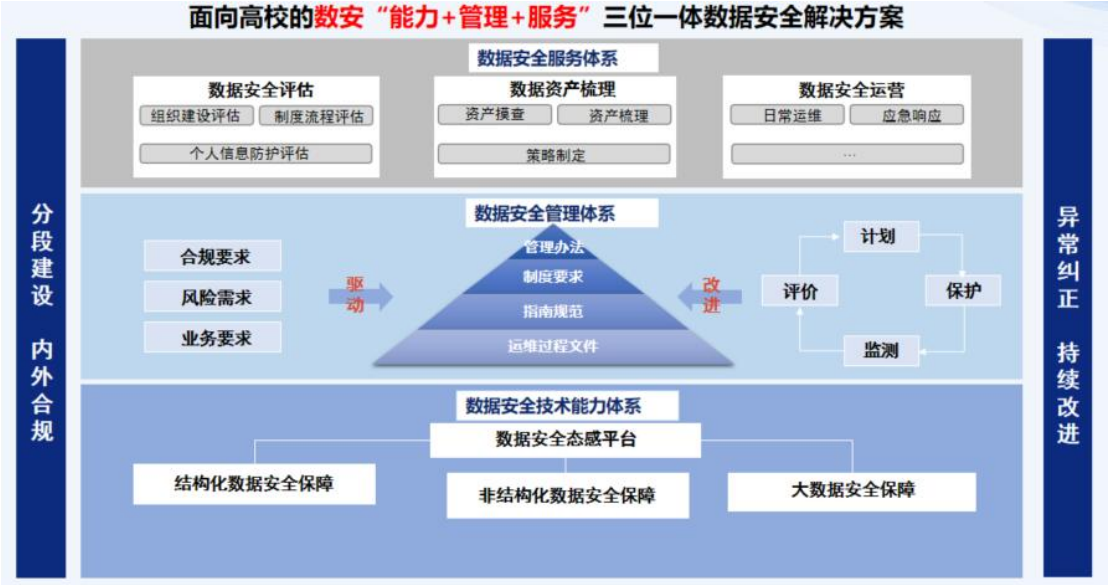
高校不同于其他行业，其自身业务系统也具备特殊的安全痛点，分析要点如下：

一是高校应用和数据是分散在数据中心的各个区域，数据暴露面大，形成的攻击面大，且各系统构建差异较大，也造成了防护的要求不同。**二是**相关的专业维护人员不足，且已有的负责网络安全的人员对于数据安全的法律法规认知和专业的知识技能掌握不到位，网安专责人员很少超过 2 人，更难以支撑起数安专责。**三是**不同形态的应用和数据会面临不同程度的数据安全风险，且在高校中重要系统有 20 多个，系统总量在 100-200，例如托管在数据中心的系统只有基础防护，相关数据又面临开发商、计算中心、所有者处室三不管的状态，数据安全依靠等保的技术数安手段，缺乏系统的数安防护能力。而且依据当前的刑法规定，系统存储敏感数据量达到 50 条以上如果发生泄露就属于情节严重。**四是**高校目前数安问题的日益紧迫且棘手的现状，数据量越来越多，敏感度越来越高，体现了数据价值也是越来越重要。数据现在成了烫手山芋，不仅法律法规在施以高压，同时愈演愈烈的数据安全事件也是令高校十分头疼的，从学校主要领导到专责技术人员，都成为被追责的对象。

3 解决方案

1、方案总览

数达安全针对高校行业的数据安全建设，以“能力+管理+服务”三位一体的思路，并利用相关技术能力，实现围绕数据全生命周期的数据安全防护。整体架构如下图所示。



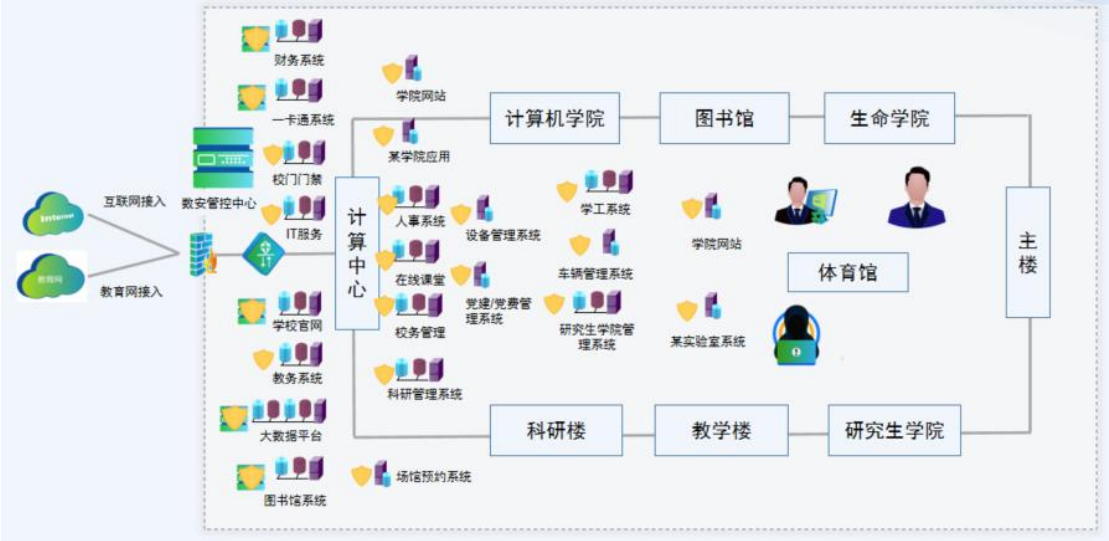
数据安全技术体系：以数据安全态感平台为中心，针对结构化数据、非结构化数据以及大数据的相关安全进行专门的保障。

数据安全管理体系：以合规要求、风险要求、业务要求为驱动，不断进行纠正、规划、执行和评价来持续改进相关的管理办法和校内的规章制度文件。

数据安全服务体系：利用数据安全评估、数据资产梳理和数据安全运营等服务构建长效化保障高校数据安全机制。

2、技术方案

针对高校我们提供了专业的技术方案解决高校当下数据安全难题。在高校计算中心搭建数安管控中心，部署数据安全服务器组，包括：数据资产管理、数据库防火墙、数据库审计、数据库加密、数据库安全运维、数据库静态脱敏及水印、数据安全态感系统、数据接口安全系统等；所有数安能力以多租户方式提供接入服务，托管系统按需租用各种数安能力服务；同时针对邮件数据安全，部署邮件安全网关，与数据资产管理进行联动，保护高校内的邮件数据安全，防止因为邮件发生数据泄露的事件。对于独立规模的系统，则单独部署相关的数安能力，按需进行。最后态势感知系统可以接收分散在其他数安系统中的状态和日志信息，实现统一展示安全态势。



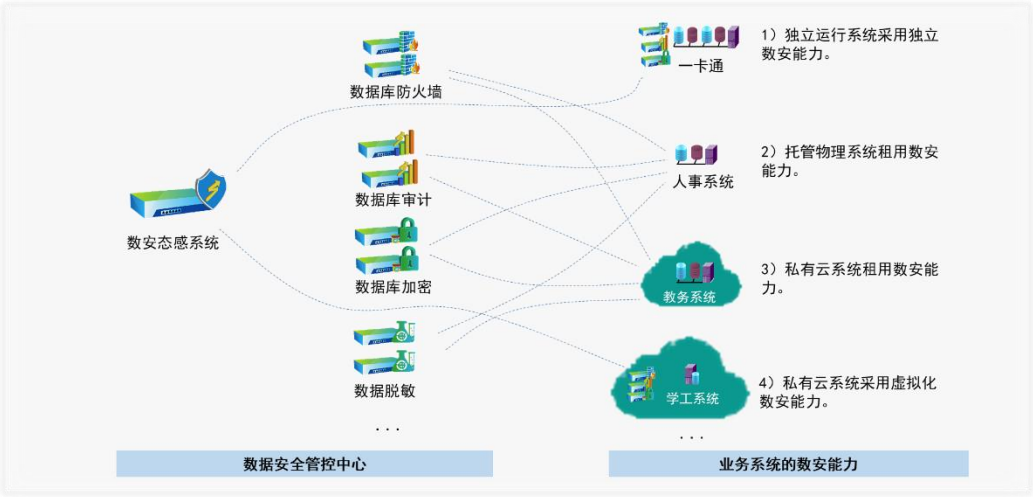
3、数安能力部署

产品名称	产品目标	产品优势
数据访问审计	数据访问行为记录、事件溯源、风险访问预警	支持大流量；审计内容更加细粒度；支持数据类型多；高性能
数据资产管理	梳理数据资产家底、建立数据分类分级台账	敏感数据识别；数据分类分级；识别、扫描数据源方式多
数据防泄漏管理	发现敏感数据以及监控数据异常流动	支持教育行业策略定向优化；泄露风险可视化；敏感数据分布全网可视化
数据库防火墙	在数据层实现数据边界的隔离，防止数据攻击	高速分析技术、多线程和缓存技术，支持高并发；快速检索、海量存储；高性能、高稳定性
数据静态脱敏	生成仿真数据，供开发测试、培训场景使用	支持多租户模式；全量水印，精准溯源；多种脱敏规则
运维脱敏	针对数据运维人员，建立安全的数据运维环境，提升运维效率	高易用性；提高运维安全；多种敏感规则，灵活的脱敏方案
数据库透明加密	实现数据的加密存储、规避 DBA 密码泄露导致的风险	敏感信息与非敏感信息的逻辑分离存储；通过密文索引在查询时能够获得和未加密相似的性能；对数据库零侵入，完全基于数据库自身的机制实现透明加密和解密，实现密文索引
数据接口安全管理	数据开放共享接口中的敏感数据，发现其中存在监测的数据安全风险	数据接口风险监测；多维度、多场景的监测和分析体系；行业定向化
数据安全态势感知	用大屏方式展示数据安全的全局态势，对所有的数据安全能力实现统一管理	数据源支持广泛；支持教育行业优化；智能分析
数据安全	自动化地开展数据安全合规性	有效支撑多部委数安考核，共完成近百次评估支

合规评估系统	评估	撑任务
数据水印与分发平台	规范数据分发流程管理、实现数据快速溯源	全量水印，支持对字符型数据任意位置插入水印；精准溯源；支持行业数据特性
数据安全应急演练	提高企业数据安全应急演练实战化、可视化和常态化的能力	快速提升企业员工实战能力；提升企业员工知识积累
数据安全风险检测	增强企业对业务数据安全风险监测的能力	提高高校自我检测手段；增强一体化监测能力；利于实现数据安全问题及时整改
邮件安全网关	满足企业邮件使用中对恶意邮件防护、邮件数据防泄漏、邮件数据留存/司法举证等场景	垃圾邮件、攻击邮件过滤与拦截；具备机器学习过滤引擎；能定位高级隐形恶意软件

4、数安中心

数据安全管控中心以态势感知系统为核心，搭建数据安全能力服务器，包括数据库防火墙、数据库审计、数据库加密、数据库脱敏等技术能力，保障托管系统及独立系统的数安能力。其中像一卡通这样的独立运行的系统，采用独立的数安能力进行防护，托管在计算中心的系统则采取租用数安能力来实现防护；而采取私有云虚拟化的系统既可以租用数安能力，也可以采用虚拟化搭建的数安能力来进行防护。所有的业务系统数据安全态势信息都会汇总到数据安全态势感知中，进行统一展示，可视化监测整体数据安全状态。



5、管理制度方案

针对高校的数据安全管理制度方案，相关制度体系需要覆盖数据全生命周期

的内部和外部场景，做好事前防范、事中管控和事后稽查与审计。事前防范中，基础部分需明确组织责任管理、人员岗位管理、数据资产管理、人员的教育培训管理、保密管理和分类分级管理；对外部则需明确数据出境规范要求、合作方调研审查的制度。事中管控基础部分要确定人员及权限管理、个人信息保护管理和合规评估管理制度，高校内部需明确数据的采集管理、传输管理、存储管理、使用管理、开放共享管理和销毁管理制度；对外同样需明确数据出境规范要求、合作方调研审查的制度。在事后稽查与审计中，基础则需具备安全审计管理、应急处置管理、投诉举报管理、监督检查考核问责管理制度，对外需明确合作方考核制度。

6、数据安全服务

6.1 数据安全评估

对于数据安全评估服务，我司人员通过访谈、文档查阅、系统查看和利用检测工具等方法调研高校内相关的保护制度、安全规划和流程，以及监管现状和当前高校具备的能力现状，进行现状的情况梳理，并利用相关的评估工具识别问题，依据问题编制整改建议，并持续跟进评估。最后结合高校当前的组织结构、人与水平、技术能力、制度情况，编写数据安全评估报告，反馈出高校的安全现状和问题及风险点，提供相关的整改建议，确定整改落实情况，给出最终的评估结果。整个数据安全评估我们将进行资产调研、威胁识别、脆弱性识别、风险评估、策略制定以及风险监测，对于基础环境的调研，我们需要了解业务系统、策略配置、当前的安全能力、账号使用情况、业务的访问流程。进而判定是否存在一系列的风险场景，确认数据的机密性、完成性和可用性是否面临威胁。

6.2 数据资产梳理

针对数据资产梳理服务，通过我们技术人员对高校的资产情况进行摸查，确定资产情况，以及敏感数据的分布情况，然后针对这些数据分阶段进行梳理，逐步细化，最后形成相应的数据资产清单，针对不同的数据形成相关防护策略，确定敏感数据情况，从而实现数据的分类分级，数据的合规管控。

数据资产梳理服务主要就解决了在高校行业，由于系统众多，数据资产理不清的情况；以及众多数据中哪些是敏感数据，这些敏感数据分布情况又是怎样的困局；还有数据是哪些人在使用，使用流程和方式是否合规，这些数据资产又是由谁在进行管理等等存在风险的场景。

6.3 数据安全运营

为了缓解高校数据安全专业人才不足的问题，我司提供专业的数安服务，保证高校在数安体系能做到建得起、用得好、管得牢。

服务分为三种类型，标准服务我们提供标准安装、调试、使用培训、系统升级服务。豪华服务则按需购买人天服务，用于交付期的集中安装、调试、规则设置，以及每周 1 天或多天定期的设备巡检、策略设置和优化、故障排查、事件溯源等服务。专属服务则包含专业技术人员进行现场值守服务，保障系统稳定运行，提供策略优化、故障排查、新增纳管、应急响应等服务，还可根据需要提供重保服务、迎检服务等内容。

4 实施方案

针对目前高校一次性预算不足以建设全部数安技术能力，我们推出了分阶段建设的方案。我们构建合规的数据安全防护体系，分为三个阶段来进行：第一阶段建立基础数据管理及差异化管控支撑能力，实现数据安全可视化、分析预警、统计报表等能力，建设数据资产管理、脱敏管理、访问和操作审计管理；第二阶段提升数据精细化管理能力，实现全局策略管理、用户行为分析、集中管控管理、接口安全监测，建设数据库防火墙、数据库加密、接口安全管理；第三阶段形成数据安全全局管理与长效运营机制，实现规范数据分发、溯源与取证、访问权限控制、风险全面感知，建设数据安全态势感知、数据库安全运维和数据防泄漏。将数据的全生命周期从事前、事中、事后形成全面的保护。

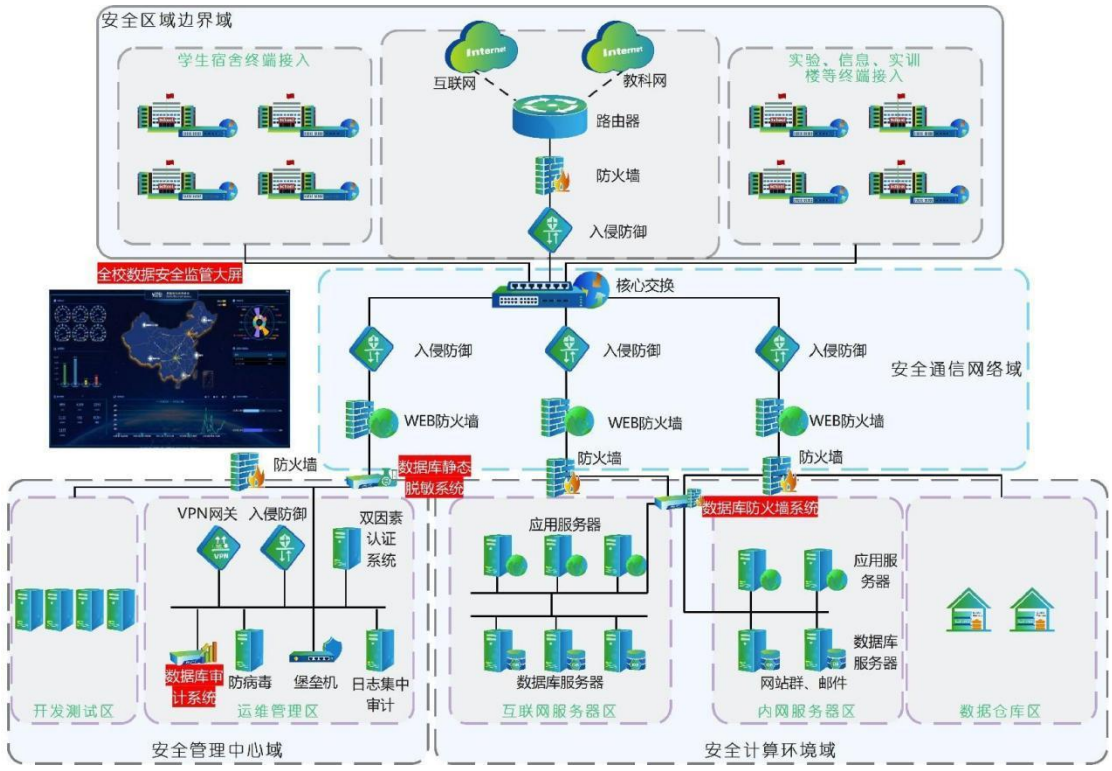
5 案例分享

本方案的全部或部分已经在如下高校应用：

案例一：南方某中医药大学案例

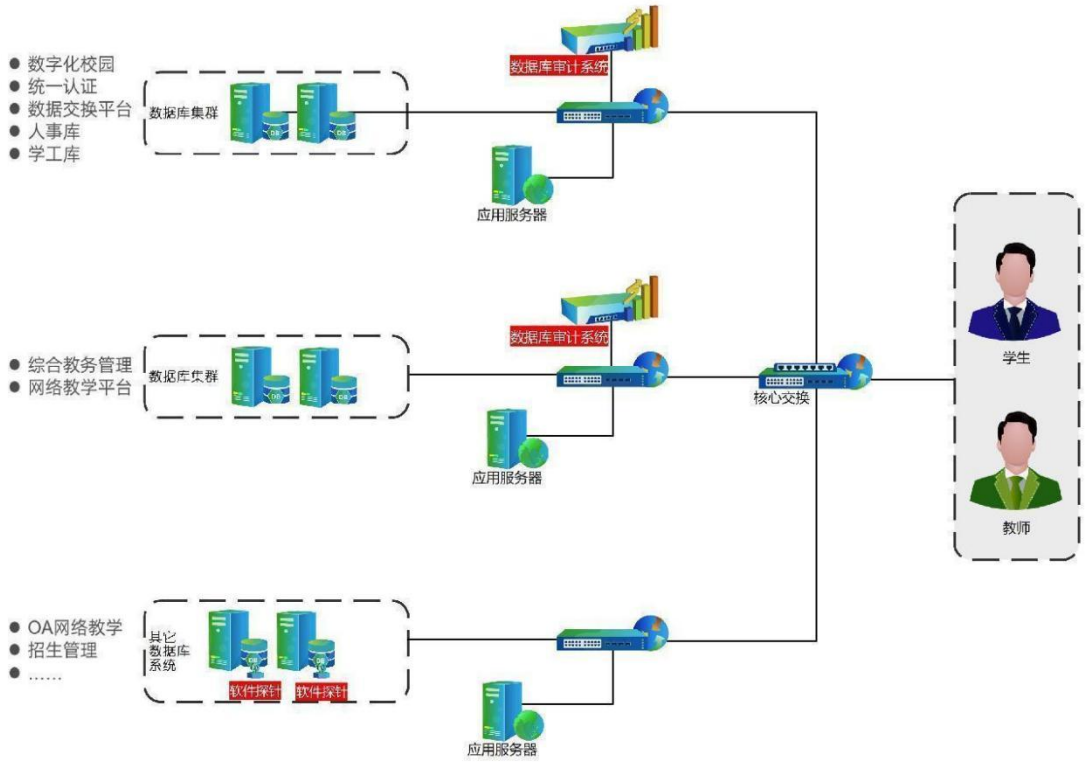
南方某中医药大学面临数据溯源追查机制缺失，且没有合规的第三方审计系统，缺乏数据访问控制的手段，无法阻断 SQL 注入等攻击数据库的恶意行为；

且校内人员在对重要数据进行开发、测试等环节上没有采取脱敏手段，而是直接使用真实数据，这个过程存在极大的安全隐患；前整体缺乏数据安全态势感知，无全局数安视野。同时该学校需要进行自身的数据梳理和数据安全风险评估，并为其制定数安体系制度，为提升相关人员技术能力也需要对人员进行培训。因此针对需求痛点，我们部署了数据安全监管平台、数据库审计、数据库防火墙、数据库静态脱敏以及提供了相关的数据安全服务，满足了该校数据审计、数据访问控制、数据脱敏、全局数据安全检测和资产梳理、数据安全评估、数安体系制度制定以及人员培训。



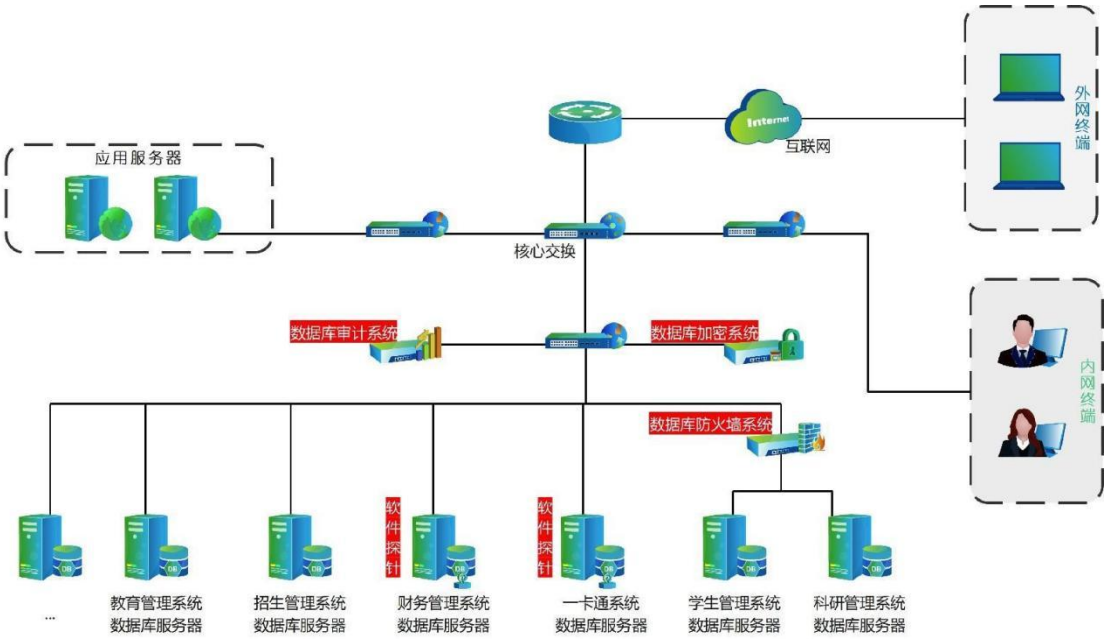
案例二：某电力大学数据库审计案例

某电力大学需要满足三级等保的合规要求，且缺乏针对校内的数据安全访问审计行为记录的手段；对于学校的教务系统、网络教学系统、招生管理系统的数据访问审计措施不充分，存在难以溯源等问题。因此部署了我司的数据库审计设备，实现了满足三级等保合规需求，也实现了数据库的状态监控，同时能够对数据库的风险访问进行实时告警，且按风险等级划分，并将每次生成的运维报表、业务报表、风险告警报表定期推送给对应部门的负责老师，实时关注学校的数据安全情况。



案例三：北京某科技学院案例

北京某科技学院要求实现数据库访问的全面审计、风险报警和事后溯源，并提供敏感数据发现能力，并对敏感信息进行加密存储，数据的访问过程要求实现异常访问的实时阻断和告警。我司通过部署数据库审计、数据库加密和数据库防火墙实现对该院校的数据保护。对所有数据库部署数据库审计产品，并针对一卡通系统，财务系统这些应用系统和数据库在同一台服务器的系统用 DB 探针的方式，实现审计功能。对学生管理和科研管理系统数据库部署防火墙，及时阻断异常的访问。对财务系统和招生系统数据库部署加密，实现对敏感信息进行加密存储。并通过独立的权限管控系统来实现对敏感数据访问的权限控制，确保其数据的安全性。最后通过开启自动学习功能，生成安全访问策略白名单。对异常访问进行及时告警或阻断，结合可视化界面和报表，实现对内部及外部人员的行为记录、访问控制管理。



6 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。