数据安全态势感知系统

产品白皮书

V4R6

重庆数达信息安全技术有限公司

2024 年 7 月

版权声明

免责条款

目录

1 引言 1
2 产品概述 1
3 产品架构 2
4 产品功能 2
4.1 集中管理 2
4.2 数据溯源 3
4.3 资产梳理 3
4.3.1 资产扫描 3
4.3.2 分类分级 4
4.4 可视化大屏 4
4.4.1 数据分布态势 4
4.4.2 用户行为态势 4
4.4.3 数据流向态势 4
4.4.4 风险告警态势 5
4.5 日志检索 5
4.6 其它功能 6
4.6.1 三权分立 6
4.6.2 单点登录 6
4.6.3 统计报表 6
5 产品部署方式 7
6 特性优势 8
6.1 大屏态势感知 8
6.2 AI 模型与画像 9
6.3 多场景多来源 9
7 产品价值 9
7.1 集中管理 9
7.2 事前预警 10
7.3 事中防御 10
7.4 事后溯源 10
8 联系我们 10

1 引言

在当代，数据库正在迅速膨胀变大，它决定着企业的未来发展。数据库作为当代信息系统的核心部件，应用十分广泛。数据库安全也十分重要，企业内部安全信息、员工或客户个人信息等敏感数据是一个企业的核心机密数据，从而要求监控与保护企业持有的数据增加开支并加大投入力度。

习总书记在 419 座谈会上提出“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设置安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力”随着《网络安全法》、《国家网络安全战略》的相继出台，态势感知被提升到了战略高度。

数据库安全态势感知旨在大规模数据环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示、分析，最终的目的是要对数据安全隐患进行决策与行动。态势感知已经成为数据安全领域聚焦的热点，代表了数据安全攻防对抗的最新趋势。

传统数据安全解决方案仅针对单节点或指定场景做定向防护，缺乏对数据整体安全态势的感知分析，帮助用户建立更完善的数据安全体系，从传统的只关注单节点侧提升至数据安全整体态势，掌握数据分布态势、数据流动态势、用户行为态势、风险分布态势。

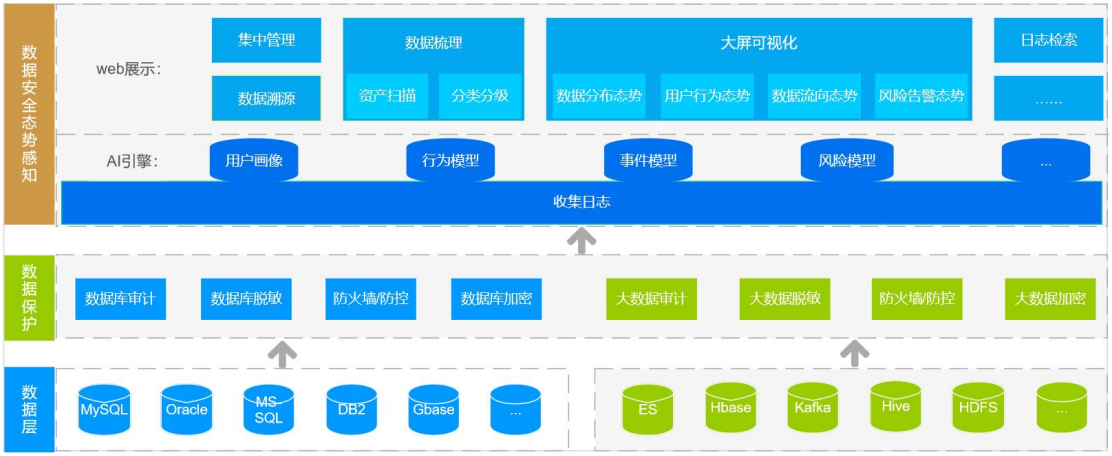
2 产品概述

数据安全态势感知系统（Data Security Situational Awareness，简称 DS-DSSA，下文均以 “态感平台”进行介绍）系统是一款以数据访问行为分析为基础的数据安全防护和管理系统。该系统通过对数据库审计、数据库防火墙、数据脱敏等各种数据安全产品采集的日志信息进行集中处理，将多种异构数据进行归一，并进行关联分析，将数据资产分布状况、敏感数据访问行为进行动态展示，并预测数据资产可能面临的泄露风险。还原并展示一个清晰、透明、可控的数据资产分布、数据访问行为、数据安全风险态势。

态感平台是一个集分析与管理为一体的数据安全感知平台，平台内置多种 AI 模型、画像、运算引擎，可对海量日志进行全量关联分析，为用户提供集中

管理、事前预警、事中防御、事后溯源服务，让用户 360° 无死角把握数据动向，辅助用户更安全有效的做出响应和决策。

3 产品架构



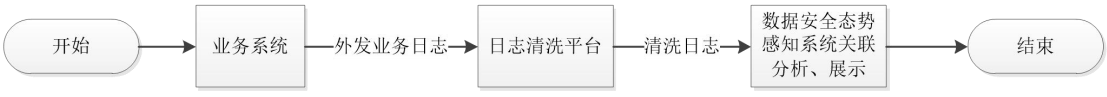
数据层为企业数据资产存储的设施集合。数据保护是通过建设各个数据安全产品对数据层中的传统数据库、大数据组件等进行安全防护，记录数据资产被访问的日志。数据安全态势感知系统支持集中管理数据安全产品，收集所有数据安全产品的海量日志，结合内置的 AI 引擎对海量日志进行全量关联分析，为企业输出可视化的大屏展示，包含数据分布态势、用户行为态势、数据流向态势、风险告警态势的可视化展示；支持泄露数据的溯源功能。

4 产品功能

4.1 集中管理

态感平台可对接我司数据库审计、数据库防火墙、静态脱敏、数据库加密产品，并进行统一集中的管理。同时支持其他公司的数据安全产品的对接模式，通过约定的规则、接口定制产品的接入方案，存在一定的定制化和适配开发工作。

1. 支持日志接入配置，汇总海量日志，为数据流动态势分析、用户行为分析、风险预警提供基础数据；日志接入业务流程如下：



业务系统将采集到的业务日志外发给日志清洗平台；日志清洗平台根据业务

系统的日志清洗规则清洗日志，例如：统一格式，填补空缺字段、删除无效数据等；清洗后的日志将写入数据安全态势感知系统，系统对日志进行关联分析，并通过可视化图表的方式进行展示。

2. 支持单点登录。当被管理设备众多时，避免管理员记录大量设备连接地址和账户密码，在记录账户密码的过程中，造成账户密码的遗失；

3. 支持数据安全产品信息的统一配置和管理。

4.2 数据溯源

通过对泄露内容特征的提取和数据库操作日志进行比对，定位泄露点节点和用户，做到事后准确溯源取证，追溯责任人，对违规和恶意攻击起到威慑，追溯的目的。录入已泄漏的数据，并提取关键字，设置溯源条件，根据泄露数据和溯源条件定位存在泄露风险的可疑数据库 IP、数据库用户等信息。

录入泄露数据：系统支持输入或导入的方式录入平台；

提取关键字：录入的泄露数据匹配内置敏感数据识别算法，提取泄露数据中的关键字敏感类型；

溯源条件：根据数据访问行为记录的日志，提供多种可配置的溯源条件，包含：数据库用户、源 IP 地址、数据库名称、时间等 17 种溯源限定条件；限定条件越详多越具体，则溯源结果越准确。

4.3 资产梳理

4.3.1 资产扫描

资产扫描通过对 mysql、oracle 等数据库中的数据进行扫描，发现敏感数据资产，梳理数据库数据结构，统计分析数据资产分布情况。

扫描数据发现敏感数据资产：系统内置了 20+种敏感数据发现规则，基本上涵盖电力、金融、公安、社保、工商、税务等各个行业的数据特征识别需求。当普通数据只在某些特殊应用系统中才具有敏感性时，我们还提供了特征字典和正则表达式两种数据匹配方式的自定义规则配置接口，满足不同数据在各类应用场景中的敏感识别要求；并且通过采集的日志分析监控数据的实时使用情况。

统计分析数据资产：统计数据库、表、字段、敏感数据库、敏感表、敏感字

段数量等；

展示数据资产分布情况：数据敏感类型分布、敏感数据类型访问量分布，敏感表数据量分布、敏感表访问次数分布。

4.3.2 分类分级

系统通过制定的分级分类方案，对数据自动标识并推荐数据分级分类标签，用户可根据系统推荐结果快速对资产进行梳理，对每个数据库的表结构，数据内容和所属分级分类信息进行相关记录，通过个各种统计分析的手段，可视化的展示数据分类分级情况，让用户更直观的了解业务场景中的数据使用情况。

4.4 可视化大屏

通过可视化的展示效果，展示企业的数据分布态势、用户行为态势、数据流向态势、风险告警态势内容。

4.4.1 数据分布态势

数据分布态势主要展示数据资产的分布情况，支持数据敏感类型分布、敏感数据类型访问量分布，敏感表数据量分布、敏感表访问次数分布等。

4.4.2 用户行为态势

分析数据库用户操作数据资产的行为日志，统计、分析数据库用户操作数据资产的规律，从中发现用户异常行为、异常用户，便于数据资产运维人员及时处理，避免数据安全事件的发生，并为修正或者重新制定数据资产安全加固方案提供依据。

统计所有用户的数量、异常数量、累计操作总数、登录总次数、登录使用的 MAC 个数、登录使用的 IP 个数等；

统计单个用户的累计操作总数、登录总次数；

分析用户的最近活跃情况、活跃规律、活跃趋势、访问的数据资产、关联账号、风险类型，在线状态情况等。

4.4.3 数据流向态势

态感平台使用各种统计、分析的方法，通过可视化的方式展示敏感数据的访问情况、数据使用过程中的流转情况，使数据资产的访问更直观清晰。

统计内容：数据访问量、数据访问次数、敏感数据访问量、访问数据的用户数量、访问数据的应用数量；

可视化图表分析：敏感数据访问量 TOP10 应用、敏感数据访问量 TOP10 数据类型、敏感数据访问量 TOP10 用户、敏感数据访问量 TOP10 IP；

流向分析：基于数据侧，监控每一条数据信息从采集，存储，治理，使用，销毁全生命的流动和调用情况，同时对数据在各个节点流转情况进行全景监控，清晰跟踪数据在地域间，组织架构间的详细的流向；支持中国地图、省市地图、企业组织架构图等 3 种数据流向图展现数据的真实流转情况。

4.4.4 风险告警态势

平台汇总接入日志，如：数据库审计、防火墙/防控、数据库加密、数据库脱敏等，通过对日志内容的解析，提取 4W1H5 个要素，从“who(谁干的)”、“where（在什么地方）”、“when（什么时候）”、“How（干了什么）”、‘what（结果怎么样）’”维度事件进行分析，发现数据在被使用过程中的各类风险事件，事件模型支持自定义添加。

通过内置风险事件模型，对如 SQL 攻击、恶意删除、恶意篡改、慢攻击等事件进行实时监控，当操作事件命中事件模型则触发告警。触发告警后，可通过下发安全策略给防火墙（如阻断某用户或某终端对某库的访问，限制访问时间等），保证数据安全。

1. 风险事件模型：支持配置操作数据资产行为的信息（例如：IP、用户名、操作类型等），定义数据资产风险事件模型。模型配置支持 30+种维度，适用于传统数据、大数据组件的事件定义；
2. 风险监控：基于配置的风险事件模型，设置事件触发频次，定义风险等级；
3. 风险告警：监测数据资产的操作日志，实时告警数据资产操作行为风险，产生告警日志。

4.5 日志检索

全场景数据快速检索能力，平台使用高效的日志管理，预处理，分布计算等

方式，针对多种维度数据实现高效检索能力，根据用户需求，提供快速检索相关数据信息的能力。

4.6 其它功能

4.6.1 三权分立

根据等级保护要求，提供管理员权限设置和分权关联，提供三权分立功能，系统可对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。

4.6.2 单点登录

平台支持单点登录方式。当被管理设备众多时，避免管理员记录大量设备连接地址和账户密码，在记录账户密码的过程中，造成账户密码的遗失。

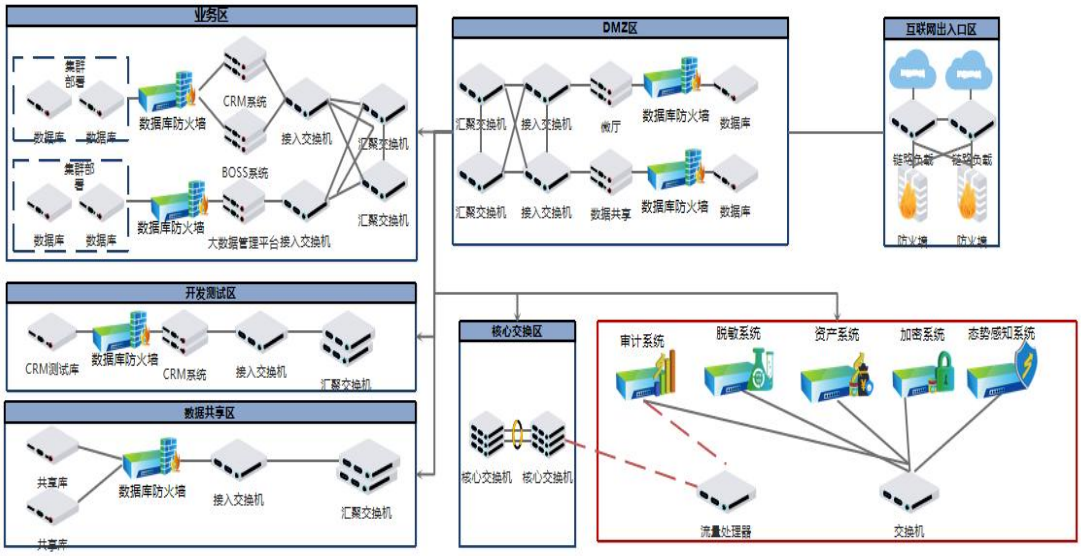
4.6.3 统计报表

对于送至平台的各种日志信息，根据分类进行统计存储。同时可基于多种维度对数据进行统计分析。

可基于：源 IP，源 MAC，数据库用户，数据库 IP，数据库，数据库表，特定敏感数据，应用服务等多维度，进行数据访问频率，数据使用趋势的统计分析，形成相关报表数据。

目前已支持账号使用情况、源 IP 访问情况、客户端工具、DDL 操作、DML 操作、DCL 操作、规则告警、SQL 平均执行时长、SQL 单次执行时长、执行次数统计、影响返回行数、高危操作统计、失败行为分析等统计报表。

5 产品部署方式



态感平台需要搭配数据库审计或者防火墙进行使用，态感平台推荐的最低配置要求如下，具体配置内容根据项目情况进行调整。

安装对象	服务器用途	推荐配置	配置说明
态势感知管理平台	用于 WEB 部署、日志统计和少量计算	CPU：4 核 内存：8G 磁盘：200G OS：CentOS7.4	高并发处理时至少 2 台服务器分布式部署
数据检索平台	用于接入日志的存储和检索	CPU：8 核； 内存：64G 磁盘：20T OS：CentOS7.4	数据检索平台设备数量等资源需要根据生产环境日产生数据量进行综合评估； 根据该数据量级可评估所需服务器资源（评估角度：数据 DPS 性能、磁盘写入性能、磁盘所需大小等）；如每天磁盘占用=每天产生数据量*0.36kb。 该配置 DPS 指标：百万级数据，200 毫秒响应结果;2 千万级数据，2 秒内响应结果；

安装对象	服务器用途	推荐配置	配置说明
数据清洗平台	用于接入日志的清洗(日志格式的转换、内容补齐、内容截取等)	CPU：4 核 内存：8G 磁盘：500G O S ： CentOS7.4	数据清洗平台需要根据接入平台数据量进行综合评估； 根据该数据量级可评估需要多少服务器资源才能及时处理。 该配置处理指标：每秒处理 22500 条数据。

6 特性优势

6.1 大屏态势感知

- **数据分布态势**

通过自研的高效数据资产发现引擎，可实现对静态数据和动态数据的发现，从冷热类型、安全等级、数据类型等多种维度构建资产分类器模型，对数据进行标识分类，实现数据资产的分级分类梳理，结合最新的大屏可视化技术输出数据资产分布态势。

- **数据流动态势**

通过自研的风险特征提取和数据资产流动分析引擎，对数据安全日志进行识别和分析实现，结合数据可视化引擎实输出数据资产的流动路径、生命周期，实现对省市县级流动趋势、业务架构流动趋势、终端访问趋势、数据自走向趋势态势感知。

- **用户行为态势**

基于 4W1H 原则(Who、Where、What、When、How)对操作日志进行全面解析，归类 sql 语句模板，提取数据库操作行为特征，根据特征识别结果对数据库操作行为进行建模和模型自优化，基于建模语句的波动情况、关联分析算法等，对数据操作行为进行有效的分析和深入挖掘，输出疑似恶意删除行为、疑似非法访问行为、疑似越权访问行为、疑似慢攻击行为、疑似拖库行为、疑似撞库等行为的态势感知。

- **风险事件预警**

通过自研的风险预警模型，对全量数据安全操作日志进行监察，实现对数据资产自身潜在风险、内部数据操作行为风险、外部攻击等多重风险因素的预警，并可通过 Syslog 等渠道进行预警推送。

6.2 AI 模型与画像

平台内置多种高危操作模型、违规操作模型、用户行为画像等，可精准发现数据被哪些用户使用，使用数据的用户做了什么。

6.3 多场景多来源

得益于平台采用的分布式架构，平台支持高可用、高吞吐场景下的日志处理，除传统的本地部署外，平台还支持公有云、私有云部署等特殊场景。

除此之外，平台内置 200 余种日志清洗规则，除对传统的审计、防火墙、访问控制、加密、脱敏等数据安全产品接入外，还可对未知数据源进行接入，用户侧只需遵照平台数据接入规范对数据进行传输即可。

7 产品价值

7.1 集中管理

平台可对业务环境内接入的数据安全产品进行集中管理，对数据安全运行状态、日志传输状态等工作相关内容实时监控，可有效避免数据安全产品出现脱管状态，实时保障数据安全。

平台除可对我司数据安全产品策略、规则等进行集中管理外，同时支持第三方产品通过平台的单点登录接口或策略接入协议进行接入管理，辅助用户更好的对安全策略、规则进行配置。

7.2 事前预警

得益于自主研发的高吞吐日志清洗、计算引擎、AI 模型与画像，平台可对海量数据安全产品日志进行全量关联分析，可感知数据在被使用或存储等场景中存在的泄露、恶意攻击、高危操作等风险并进行预警。

7.3 事中防御

在感知到数据存在的潜在风险时，可通过平台数据资产分布管理快速定位数据资产，配合策略、规则管理，数据安全产品集中管理等功能，快速对风险进行封堵，从而避免数据泄露事件的发生。

7.4 事后溯源

平台运用大数据分析可做到对数据全链路的监测，即使数据发生泄露，也可回溯数据泄露的源头，找到数据泄露的人员或终端，做到有迹可循，有证可查。

8 联系我们

地址：
电话：
网址：
邮箱：
微信公众号：