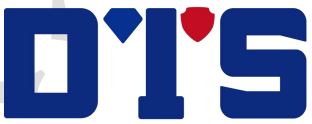
数据库防火墙系统产品白皮书

V4R1



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

目录

1 概述/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，国与国竞争日趋多元化和白热化，正在重塑全球政治经济格局。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。

2021 年 7 月 2 日，国家网信办发布公告称，为防范国家数据安全风险，维护国家安全，保障公共利益，网络安全审查办公室按照《网络安全审查办法》，对“滴滴 出行”实施网络安全审查。7 月 4 日晚，国家网信办发布通报称，根据举报，经检测核实，“滴滴出行”App 存在严重违法违规收集使用个人信息问题，通知应用商店下架“滴滴出行”App。2022 年 7 月，滴滴因此被罚款 80 亿元。

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、销毁等多个阶段，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。

数据采集阶段：存在管理制度不规范、采集策略不合理、缺乏采集监控等，导致未授权采集、过度采集、数据倒流等风险。

数据传输阶段：存在敏感数据未加密传输、缺乏数据流动监测、缺乏溯源手段等问题，导致数据泄露和非法篡改等风险。

数据存储阶段：存在敏感数据明文存储、数据备份与恢复能力欠缺等问题，导致数据泄露、篡改破坏、丢失、无法复原的风险。

数据使用阶段：存在未建立数据访问控制机制和数据风险检测机制等问题，导致数据使用不当或被恶意盗取、篡改破坏的风险。

数据共享阶段：存在数据共享接口安全管控能力不足、数据脱敏能力缺失、数据溯源能力缺失等问题，导致数据未授权提供、超范围公开、再共享等风险。

数据销毁阶段：存在销毁技术手段不完善、缺乏销毁管理措施等问题，导致残余数据利用和残余介质利用的风险。

共性风险：除上述各个阶段之外，组织因缺乏数据梳理和数据分类分级能力造成敏感数据的失管和泄露、缺乏整体数据安全态势感知和数据安全监测评估能力导致企业无法进行整体的数据安全监测预警和风险评估。同时，因误操作、权限滥用、恶意窃取以及内外部联合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**共性风险。**

1.4 相关法律法规

《网络安全法》对数据安全保护提出了新规定和新要求，特别是其中涉及的个人信息保护、跨境数据传输评估等方面，明确提出了网络运营者（包括关键信息基础设施的运营者）的安全保护义务之一是防止网络数据泄露或者被窃取、篡改。

《数据安全法》中规定开展数据处理活动应当建立健全全流程数据安全管理制度、组织开展数据安全培训、采取相应的技术措施、加强风险监测等。发生数据安全事件时，应当立即采取补救措施并按照规定及时告知用户并向有关主管部门报告。

《个人信息保护法》中规定，个人信息处理者应履行必要的数据安全保障义务以及其他基本法定义务。如发生个人信息泄露、篡改、丢失的，数据处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

《网络安全等级保护条例》（等保 2.0）的相关规定中，数据安全是核心内容之一。在原有等保 1.0 对数据安全的要求基本不变的情况下，根据新计算环境和业务场景对数据安全保护能力做出了更贴合实际情况的明确要求。数据安全的测评指标主要来自于通用要求的“安全计算环境”部分，其中对数据访问的审计、访问控制、加密都有要求明确要求，并且在附录部分大数据应用场景说明中对脱敏和溯源也进行了相关规定。

《关键信息基础设施安全保护条例》要求运营者在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

《民法典》人格权编第 1038 条规定，信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供个人信息，但是经过加工无法识别特定个人且不能复原的除外。

1.5 需要增强的数据安全访问控制

现有的边界安全防护产品均采用协议识别、连接状态检查等技术路线，可以建立起网络的安全边界，但是由于数据是流动的，无法建立起数据的安全边界，也就无法解决数据层的越权访问、SQL 注入、漏洞攻击等安全威胁。承载数据的

IT 系统需要增强的数据安全访问控制设备，以解决数据层面的安全问题。

2 产品简介

数达安全数据库防火墙系统（简称 DS-FW），是一款基于数据库协议分析与访问行为控制的数据库安全防护产品，由数达安全公司研发并具有完整的自主知识产权。

DS-FW 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，实现数据库的行为特征分析、访问行为监控和危险操作阻断。从数据源头上解决数据操作过程中所面临的各样数据安全问题，有效满足内部安全保障需求及外部国家合规安全管理规范要求。

DS-FW 系统能够通过学习期对用户操作行为特征的提取、分类和整理，形成用户行为画像，即时建立每个用户的访问行为特征模型。通过该模型，不仅能够极大地减轻数据库安全防护策略的配置工作量，而且能够精准识别数据库账户被盗用带来的攻击威胁，实现主动防护。

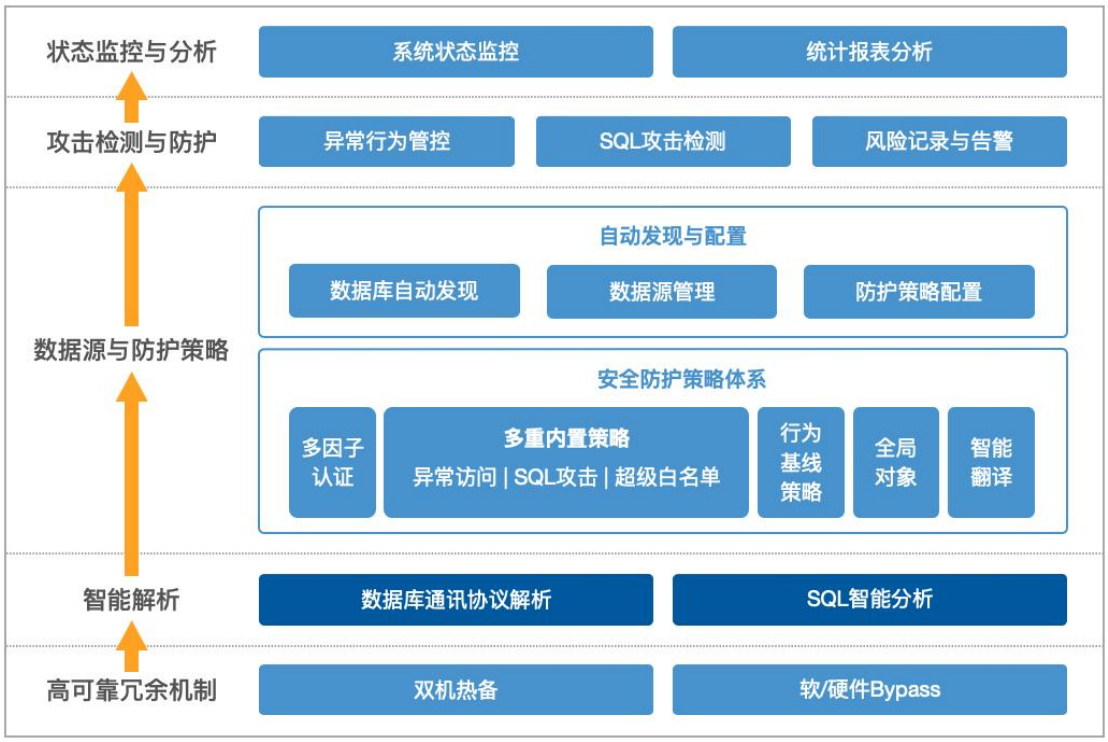
DS-FW 系统具备异常行为、SQL 注入攻击和缓冲区溢出等的检测防护能力，并结合多因子身份鉴别机制，能够帮助用户抵御来自外部的各类攻击行为，同时有效控制内部用户的越权等非法操作，为用户业务稳定和数据安全保驾护航，并快速地满足合规要求。

DS-FW 系统采用串联的方式部署在数据库服务器和应用服务器之间，能够屏蔽直接访问数据库的通道，防止数据库节点被各类攻击者、扫描工具发现，从而诱发的各类攻击行为，保证核心业务安全、平稳地运行。系统支持“透明直路”、“旁路代理”等多种部署方式，结合双机热备、负载均衡等部署模式，以及软/硬件 Bypass 功能，能够保证业务运行不中断，提高系统的高可靠性。

DS-FW 系统具有平台化、智能化、高可靠、高性能的特点，能够广泛应用于金融、电信、互联网、医疗等行业领域，以及政府部门、军工、涉密单位等。

3 产品架构

DS-FW 系统结构分为五大部分，如下图：



- **高可靠冗余机制：**通过双机热备和软/硬件 Bypass 的多重机制，实现高可靠冗余特性，保障业务连续运行；
- **智能解析：**对抓取的数据流量包进行数据库通讯协议解析和 SQL 智能分析；
- **数据源与防护策略：**自动用户网络中的数据库节点，并对其进行数据源管理；根据不同的数据库厂家，预定义了不同的规则体系，帮助用户提升策略配置的有效性；
- **攻击检测与防护：**实时监控数据库访问行为，根据预定义策略进行精准化策略匹配，能够及时发现异常行为、SQL 攻击等风险事件，并对其进行风险记录与阻断告警；
- **状态监控与分析：**对系统的运行状态、数据库业务的各项指标进行可视化监控，以及对风险事件进行细粒度的统计分析。

4 功能特性

4.1 高可靠冗余机制

系统提供透明部署模式下的多重高可靠冗余方案：

- 系统采用双机部署时，系统能够实时同步各类安全策略配置，当主机出现异常时触发主备切换，保持业务流量不中断；
- 系统采用单机部署时，当系统出现异常，通过软/硬件 Bypass 功能，能够及时导通业务通道，防止系统出现单点故障导致的业务中断。

4.1.1 双机热备

系统能够支持基于主备模式和负载均衡运行模式下的双机部署方式，以应对数据库多链路冗余组网下的部署。

- 两台设备通过心跳网口发送 KeepAlive 心跳报文进行主备间探测与切换，并采用会话同步、策略同步机制，保证双机之间的一致性，保障系统的连续防护能力；
- 当数据库采用集群、多链路冗余部署时，系统可以通过负载分担的部署方式，为每一条业务链路提供单独的保护能力。

4.1.2 软/硬件 Bypass

系统实时监控网卡的运行状态，具备硬件断电 Bypass 和软件异常 Bypass 导通能力，具体包括：

- 在进程挂死、CPU 使用率超限等特定条件下的自动 Bypass 能力，能够有效防止单点失效，保障业务流量不中断；
- 在业务流量接近或超过设备的处理能力时，可以通过配置，将一部分流量智能放行，达到部分 BYPASS 的效果，以避免造成严重的业务阻塞；
- 手动启动 Bypass 能力，在应急情况下导通网络通道，避免异常阻断。

4.2 智能解析

数据库通讯协议解析，是数据库安全关键技术中的核心部分，其准确度和全面度直接关系到防火墙产品的效果。

DS-FW 系统具备多种类型的数据库通讯协议解析能力，能够实现包括参数化的 SQL 语句、嵌套 SQL 语句和各种长 SQL 语句的精准解析，并通过将解析出的 SQL 语句与 SQL 注入特征库、漏洞库等进行模式匹配，准确发现高危操作或攻击行为，为系统防护提供风险拦截和实时报警的技术基础。

4.3 数据源与防护策略

4.3.1 数据源管理与配置

系统采用全部放行的默认策略，可以帮助业务系统的快速接入，减少因为安全策略配置而导致的业务系统中断风险。通过快捷的风险访问策略设置，实现对数据库访问行为的实时监控。

系统提供策略同步功能，一次配置即可将策略下发给相同类型的所有业务系统使用，减少应用于数据库集群时的策略配置工作量。

4.3.2 安全防护策略体系

系统结合多年数据安全经验和大量客户需求，基于 TCP/IP 协议栈模型，并根据数据库的访问行为特征及不同数据库类型的特点，为用户提供了多层次、精细化的数据库安全防护策略体系，使数据库的安全防护级别达到最高等级。

4.3.2.1 多因子认证

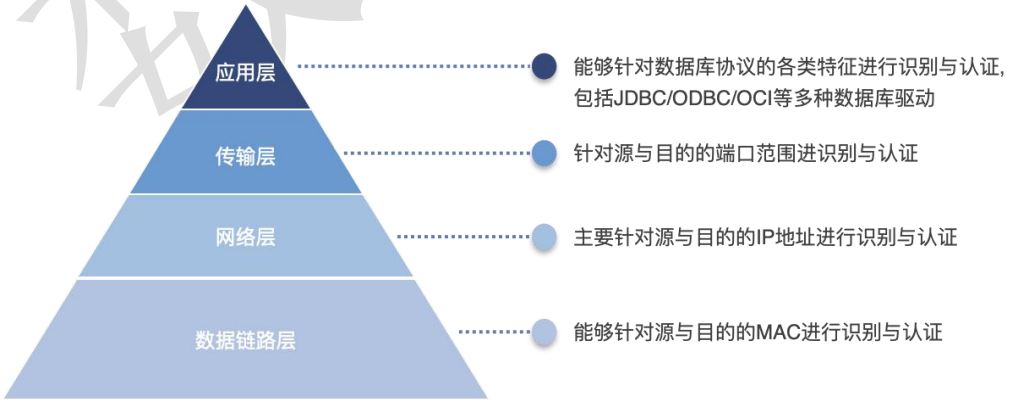
系统采用多因子的组合认证方式对访问者进行身份鉴别，能够弥补单一的“用户名+密码”认证方式安全性的不足，同时满足合规要求。

应用程序对数据库进行访问时，必须经过数据库防火墙和数据库自身的多重认证，包括但不限于：时间（访问时间）、来源（数据库用户、访问者主机 IP、主机名、主机系统用户、客户端应用程序）、行为（访问对象、操作类型、其他行为特征）。

系统支持通过多因子组合方式，预定义包括白名单、风险监控和黑名单三种类型的防护策略：

- **白名单：**被判定为无风险的访问行为的集合；
- **风险监控：**被判定为存在一定风险的访问行为的集合；
- **黑名单：**被判定为高风险的访问行为的集合。

基于多因子认证方式，可实现 TCP/IP 网络协议层面的协议栈防护机制：



4.3.2.2 多重内置策略

- **异常访问**

系统内置上百种异常操作行为特征，包括脱库、撞库、删表等高危操作，以

及批量数据篡改、大规模数据泄露等风险行为类型。

启用异常访问策略，系统能够针对不同的数据库访问来源，提供对数据的访问权限、操作权限等的有效管控。结合对 NO WHERE 语句的风险判断，避免大规模数据泄露和篡改。

- **SQL 攻击**

系统采用主动防御机制，内置基于 SQL 注入和缓存区溢出特征库等数据库漏洞库，提供对 SQL 注入等漏洞特征检测和防御能力。内置特征点超过 500 个，基本能够识别常见的漏洞攻击行为。

启用 SQL 攻击策略，当发生 SQL 注入或其它漏洞攻击行为时，系统能够实时捕获到对应的 SQL 语句及相关会话信息，基于精准的 SQL 语法分析，系统可以准确定位 SQL 语句中的操作谓词和常量表达式，保障注入、攻击行为识别的准确性。

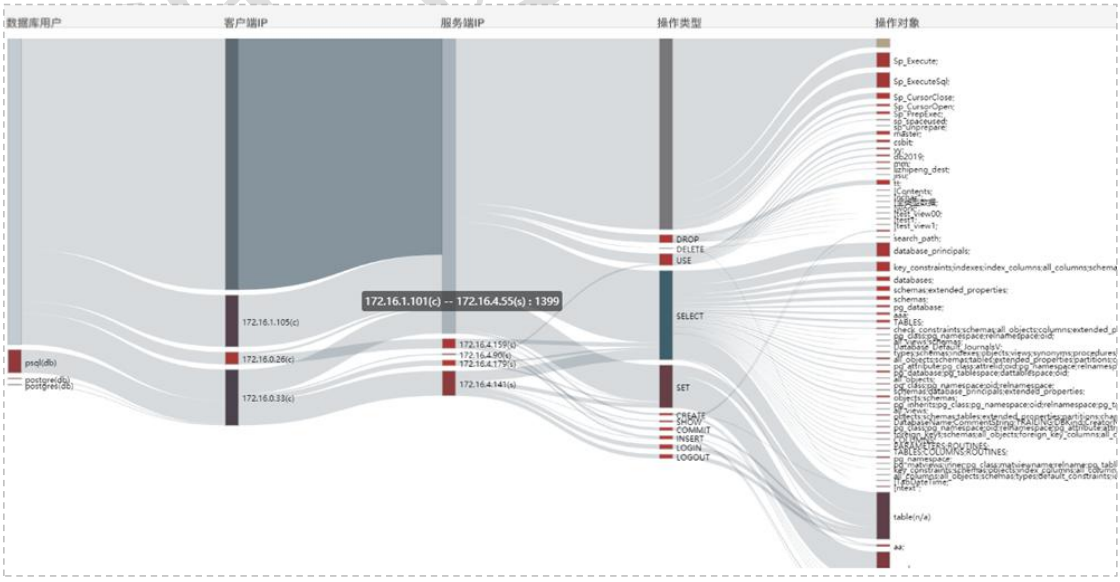
- **超级白名单**

系统将一系列无风险的高频 SQL 操作进行汇总，并内置形成超级白名单。例如，使用数据库连接工具（例如 SQL Developer）登录数据库时会对数据库发送设置环境信息的 SQL 语句，这些操作通常是没有风险的，不需要进行监控。

启用超级白名单，将会屏蔽此类信息，显著减少日志中的干扰项，提高日志的价值，并能一定程度上缓解存储压力。

4.3.2.3 行为基线策略

系统能够通过自定义学习期，对包括业务操作、特权操作和工具操作的数据库访问操作，按照访问来源、访问途径、访问对象、操作行为、操作次数等维度对其进行自动学习，完成语句、会话的建模分析，形成用户行为的基线策略，构建数据库安全防护基础模型。



启动行为基线策略后，系统将提取用户的访问行为特征数据，通过检查访问行为与基线的偏差来识别风险，对偏离基线的操作行为进行风险告警，并根据预定义的处理方式，对偏离基线行为进行风险阻断。

行为基线策略不仅能够对合法账号实施的非法行为实现精准识别，提高系统

的安全防护能力，而且能够避免规则的复杂配置，减少人工压力。

4.3.2.4 全局对象

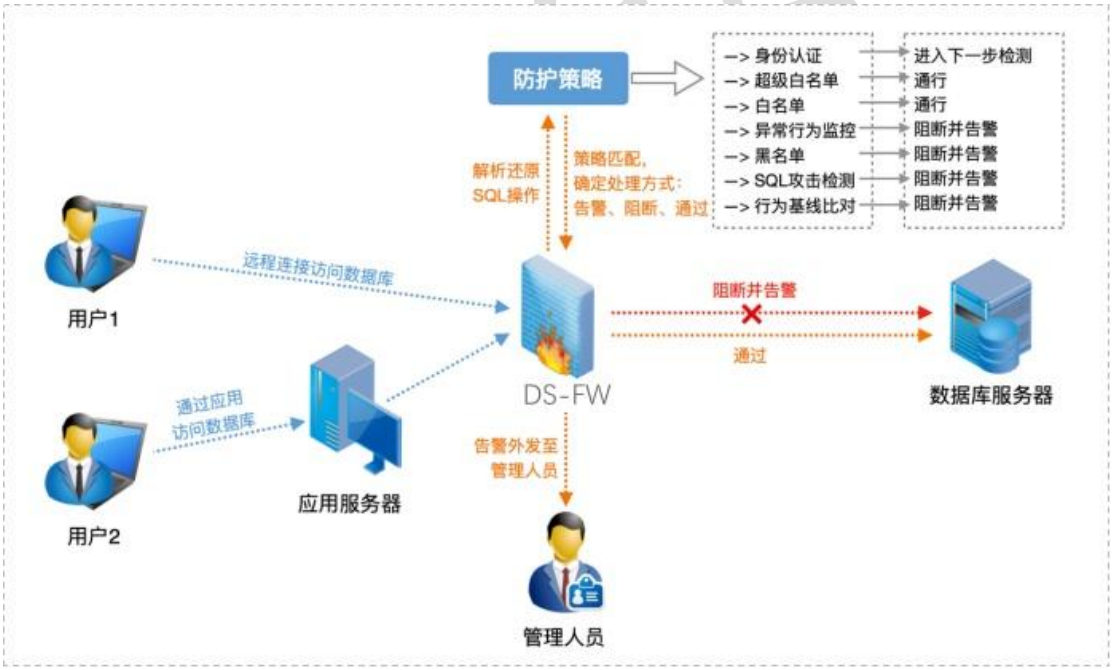
系统为策略提供了全局对象特征库，支持客户端 IP、工具名称、OS 用户、数据库用户、表名、列名、SQL 关键字、时间范围等多种全局对象的特征配置与管理。通过自学习的方式提取各类数据库行为的特征并生成全局对象，用户可以根据实际需要直接选取，方便在策略配置中直接引用，大大提升策略配置的效率。

4.3.2.5 智能翻译

系统提供基于 SQL 类型、表和字段的智能翻译功能，能够根据定义的翻译字典内容，自动将日志中的 SQL 语句翻译地更加贴近业务，便于用户对于风险日志的理解，了解风险事件内容。

4.4 攻击检测与防护

系统跟进启用的策略，对访问数据库的网络数据包进行实时的监控分析和策略匹配，能够识别数据库的异常访问和攻击行为，及时进行会话级阻断，从而有效保护核心数据的安全。



4.4.1 异常行为管控

系统能够实时监控数据库的连接信息、风险状态等，并对数据库的各类用户行为进行严格的监控和管理，及时阻断未经授权的数据库连接和操作，防止内部攻击或者越权操作行为的发生。

系统通过内置各类数据库的异常访问行为特征库，能够有效的阻止数据库被拖库、撞库、批量篡改数据、批量删除数据等严重安全事件的发生。

4.4.2 虚拟补丁

数据防火墙虚拟补丁通过控制对数据库的输入和输出，检测其会话信息和语句信息对漏洞的尝试利用，阻止或消除漏洞攻击行为。

- 虚拟补丁是在数据库外架设一个安全层，无需升级数据库补丁，即可有效防止漏洞攻击；
- 虚拟补丁集成在防火墙上，更新完善过程并不会对业务系统造成影响；
- 数据库防火墙系统通过自动学习完善基线策略库，形成主动防御，与漏洞库搭配实现虚拟补丁防护。

4.4.3 风险记录与告警

系统能够对命中策略的数据库风险访问行为日志进行汇聚、查询和告警处理，满足客户对突发事件的即时知情需求。

具体包括：

- 对风险告警进行分级、分类等聚合统计，方便用户对告警信息的查看、管理和风险趋势的预判；
- 支持对告警日志的查询统计和误报处理，从而提高告警日志的准确性和可读性；
- 提供 Syslog、Email、FTP、SNMP、短信等多种告警日志外发方式，使用户在非登录状态下能够及时收到告警信息。

4.5 状态监控与分析

4.5.1 状态监控

系统将防护时间、风险统计、会话统计、网络流量统计、资源使用率、Bypass 状态等自身的防护状态进行了集中可视化展示，能够使用户对系统当前运行状态和防护情况一目了然。

4.5.2 统计报表

系统监控防护状态，生成风险实时报表，能够直观了解到各类风险事件的发生情况。

数据库防火墙提供《场景的操作异常分析》《来源的风险行为分析》《操作的风险统计分析》《结果的风险防护分析》等丰富的报表模板，并支持自定义报表的统计维度。通过选用报表模板发起执行报表任务，能够实现对风险日志及阻断行为进行各种粒度的报表输出、统计趋势展示等，以真实的反应数据库的业务运行状况、数据安全风险情况等。

- 报表预览根据系统内置的报表模板将对应的日志进行统计展示，提供分析数据的能力，同时提供清晰的信息便于阅读和图形的可视化展示。
- 支持邮件定期发送报表，有利于观察、分析数据的动态。

4.6 敏感数据发现

系统通过内置敏感数据识别规则，能够识别用户数据库中的敏感数据，提供敏感数据的分布报告，方便用户针对敏感数据制定访问控制策略。

5 典型部署

5.1 直路透明模式

将 DS-FW 设备物理串联数据库节点之前，所有用户访问的网络流量都串联流经设备。通过透传技术，应用端看到的数据库地址不变，且在数据链路层，数据帧的源和目的 MAC 均不会被改变。

直路透明模式部署图

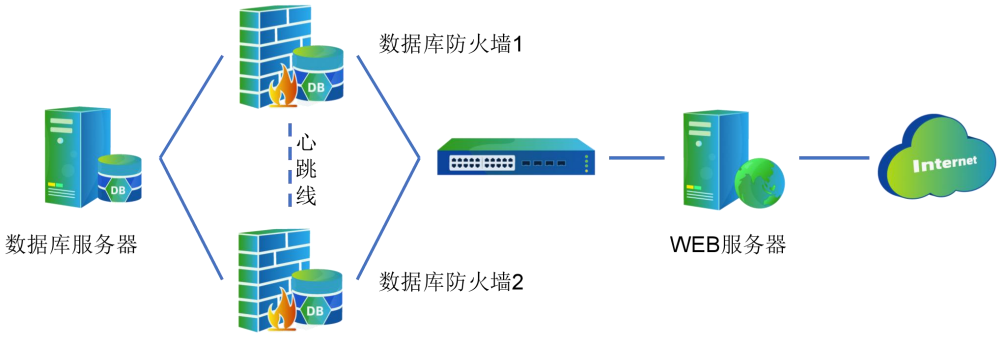
5.2 旁路代理模式

将 DS-FW 设备旁路接入数据库所在网络，各类应用采用将数据库连接指向数据库防火墙设备地址，所有访问数据库的流量都经过防火墙设备的过滤和转发。通过代理接入模式，网络拓扑结构不变，尤其适用于云计算和虚拟化环境。

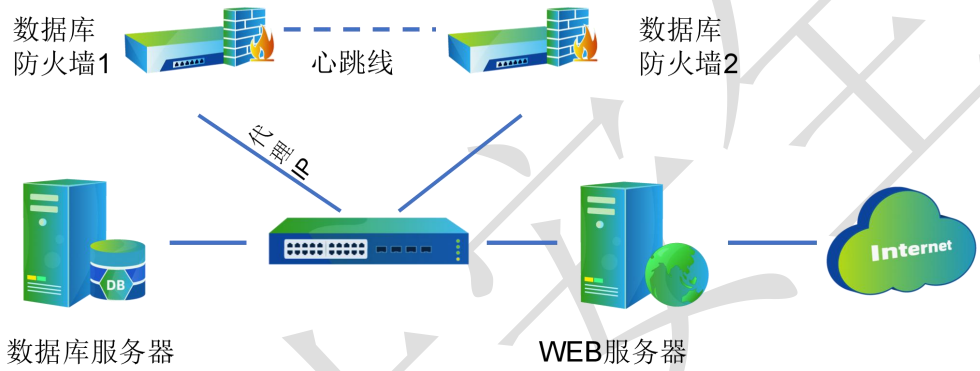
旁路代理模式部署图

5.3 双机热备模式

将两台 DS-FW 设备串联接入用户网络，设备之间通过心跳信号进行探测监控与切换。当单台设备出现异常，可以快速地将业务流量切换到对端设备。系统基于会话同步和策略同步机制，保障两台设备之间的信息同步。



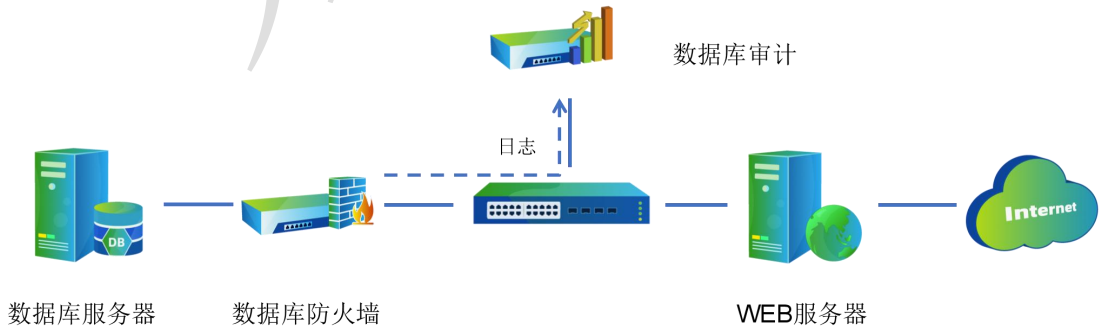
直路透明模式下双机热备部署图



旁路代理模式下双机热备部署图

5.4 混合部署模式

将数据库防火墙接入数据库所在网络，客户端逻辑连接防火墙设备地址，所有对数据库的访问流量都流经该设备进行过滤和转发。同时将日志发给审计系统，与审计系统配合使用，对数据库进行审计与防护。



混合模式部署图

6 产品优势

数达安全数据库防火墙系统在产品成熟度、专业度、可发展性等方面优于业务友商。在功能完备性、SQL 处理能力等方面处于领先地位。在数据安全深化应用，数据安全治理体系建设结合方面，具有一定超前性。

6.1 全面的策略体系

数据库防火墙区别于网络防火墙，具有网络和应用行为的多个层次的全面防护体系。不仅能够在 TCP/IP 协议栈的 2-4 层上对源和目的的 IP、端口号、MAC 等进行访问控制，更能够实时监控数据库操作行为，对 SQL 注入攻击和异常访问等进行风险鉴别和非法阻断。

6.2 细粒度的访问控制

系统采用多因子的认证方式，对数据库访问者的身份进行多重鉴别。能够实现对数据库访问行为的访问时间、访问来源、使用工具、目标对象以及具体操作进行多层次的识别和认证，访问控制粒度更全面、更精细。

6.3 高可靠的冗余特性

保障数据库正常业务的有效运行，是防火墙产品的首要任务。DS-FW 系统具备多重链路冗余机制，实现高可靠的部署特性。

- **双机热备**

系统支持双机主备部署，可高效融入用户已有网络拓扑。两台设备通过 HA 心跳线进行主备间探测，网络异常时能够实现秒级切换，保证业务流量正常运转。

- **软/硬件 Bypass**

系统实时监控网卡运行状态，能够在进程挂死、CPU 使用率超限和网卡瞬时流量超限等特定条件下的自动 Bypass，防止单点失效，保障业务流量不中断；在业务流量接近或超过设备的处理能力时，可以通过配置，将一部分流量智能放行，达到部分 BYPASS 的效果，以避免造成严重的业务阻塞；而且能够在应急情况下手动触发 Bypass，导通网络避免异常阻断。

6.4 强大的协议兼容性

系统支持 OCI/JDBC/OLEDB/ODBC 等常见协议，能够支持 Oracle、MySQL、MSSQL、Sybase、DB2、达梦 6/7、人大金仓、神州通用、InforMix、PostgreSQL、Gbase、Hive、MongoDB、Redis、TeraData、Cache、Kafka、ElasticSearch、HANA、MariaDB、Hbase 等多种数据库类型，几乎涵盖了所有的关系型数据库和主流的大数据平台，兼容性强。

6.5 安全易用的处理机制

- 使用高性能硬件平台、内核优化技术，满足高负载环境下的性能要求；
- 智能学习，对数据库访问语句自动进行模式提取与分类，并生成特征模

型，避免规则的复杂配置；

- 纯透明的部署方式，应用程序的使用环境以及授权用户的数据库操作管理过程均不会被改变。

6.6 高性能处理机制

- 网络吞吐量：12Gbps
- 纯数据库流量：1100Mbps
- 处理能力（平均长度比例）：12 万 SQL/s
- 会话新建能力：20000session/s
- 会话并发能力：240000session/s
- 日志检索速度（带通配符模糊检索）：<1min，1 亿记录

7 产品价值

7.1 应对外部攻击威胁

外部黑客利用软件缺陷或潜在漏洞，能够通过 SQL 注入或漏洞攻击入侵目标系统，致使数据库泄漏、账号盗取、系统瘫痪等。

系统通过内置基于 CVE 的 SQL 注入&缓冲区溢出特征库，能够快速有效地识别 SQL 注入攻击、缓存区溢出等风险，并及时进行拦截阻断，有效应对数据库被攻击的威胁。

7.2 应对内部访问风险

DBA、研发人员等内部权限用户，能够直接访问数据库，有意无意的高危操作或越权访问，易对数据库造成破坏。

系统通过内置和自定义的访问控制规则，并结合黑白名单屏蔽处理机制，能够有效防范内部人员泄密、违规备份、权限滥用等访问风险。

7.3 事前策略设置

系统提前设置防护策略，为风险行为防护做好准备。

7.4 事中告警阻断

告警阻断威胁到数据库数据财产安全的风险行为，保证威胁数据财产安全的操作无法到达数据库。

7.5 事后审计溯源

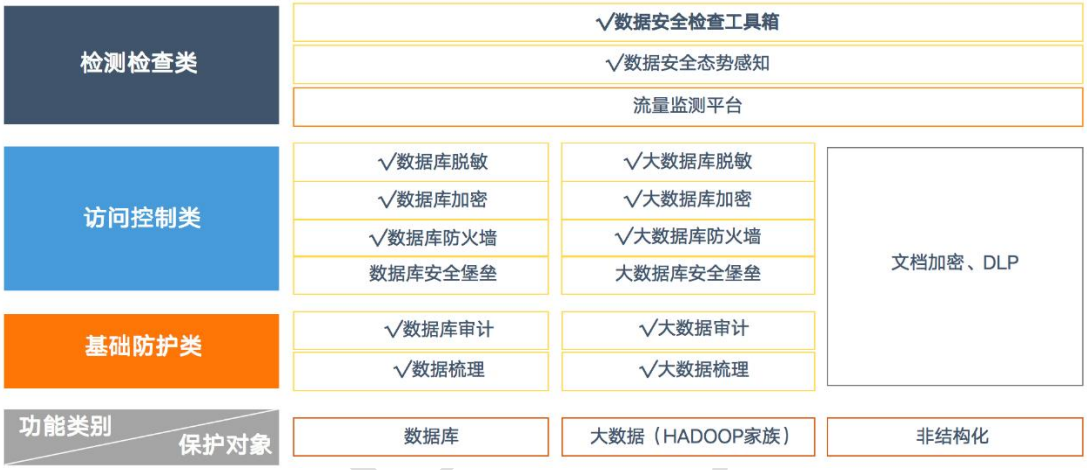
系统能够通过对风险行为进行 Syslog、SNMP、邮件、短信等方式的告警，并记录风险访问行为日志，便于事后追踪分析，解决数据库风险难以追踪溯源的问题。

8 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北京、上海、深圳等全国二十多个省设置了办事处，服务全国客户。