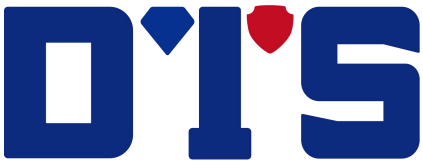
数达安全

数安卫士产品白皮书



重庆数达信息安全技术有限公司

2024 年 8 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

前 言 1
1 概述/背景 2
1.1 数据资源成全球博弈主赛道 2
1.2 全球重大数据泄露事件频发 2
1.3 数据安全面临的主要风险 2
1.4 相关法律法规 3
1.5 数据库加密需求 3
1.5.1 数据安全合规要求 3
1.5.2 业务安全需求 4
2 产品概览 6
2.1 产品目标 6
2.2 产品原理 ..... **错误！未定义书签。**
2.3 产品架构 6
3 产品功能 8
3.1 敏感数据发现 8
3.2 加密和解密 ..... **错误！未定义书签。**
3.3 增强访问控制 ..... **错误！未定义书签。**
3.4 系统安全 16
4 产品特点与优势 18
4.1 高性能 ..... **错误！未定义书签。**
4.2 高可靠性 18
4.3 易用性 18
4.4 强大的兼容性 18
5 典型部署 19
5.1 软加密部署 ..... **错误！未定义书签。**
5.2 硬加密部署 ..... **错误！未定义书签。**
6 产品规格 20
7 产品价值 21
7.1 满足合规要求 ..... **错误！未定义书签。**
7.2 提升数据安全治理能力 ..... **错误！未定义书签。**

7.3 提升经济效益 21
8 公司介绍 22

前 言

近年来，以 5G 技术、数字化、智能化为主要特征的新工业革命蓬勃兴起，推动我国产业结构深刻变革。数据作为创新发展的基石，已成为国家基础性战略资源和驱动行业转型发展的重要引擎。随着全球数据呈现爆发增长和海量集聚，为人类带来无限发展机遇的同时也带来了新的安全风险和挑战，严重影响国家安全、经济发展、社会稳定和个人权益。

在此背景下，数据安全的重要性被提到了前所未有的高度。我国积极加强数据安全管理布局，《网络安全法》、《数据安全法》、《个人信息保护法》与《关键信息基础设施安全保护条例》的相继出台，全面构筑了中国数据安全领域的基础法律框架。继上述四个国家级法律之后，各行业陆续出台了本行业配套的法规、标准、指南。为我国企业落实数据活动主体义务与责任提供了法律依据。

为解决数据安全领域中的中小企业数据库安全的突出问题，数达安全在国家政策、法律法规、行业监管等基础上，针对当前中小企业普遍面临的数据安全风险现状、治理困境等，研发了数安卫士产品，以完善数据安全管控体系，为关键信息基础设施保驾护航。

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 数据库数据安全保护需求

1.5.1 数据安全合规要求

《数据安全法》第二十七条规定：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。

《网络安全法》第二十一条规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和**加密**等措施；

《个人信息保护法》第五十一条规定：个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

《网络安全等级保护条例》第二十条规定：网络运营者应当依法履行下列安全保护义务，保障网络和信息安全：

（六）落实数据分类、重要数据备份和加密等措施。

《密码法》第二十七条规定：法律、行政法规和国家有关规定要求使用密码进行保护的关键信息基础设施，其**运营者应当使用密码进行保护**，自行或者委托密码检测机构开展密码应用安全性评估。

《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》第六章：数据采集安全安全 PA01 数据分类分级：“基于法律法规以及业务需求确定组织内部的数据分类分级方法，对生成或收集的数据进行分类分级标识。应对不同类型和级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施（BP.01.07）”。

《GB/T 40050-2021 网络关键设备安全通用要求》第五章 安全功能要求 5.9 数据安全：“要求网络关键设备应具备防止数据泄露、数据非授权读取和修改的安全功能，对存储在设备中的敏感数据进行保护”。

第六章 安全功能要求 6.3 运行和维护：“应为用户提供对废弃（或退役）设备中关键部件或数据进行不可逆销毁处理的方法”。

1.5.2 业务安全需求

数据库中如果存储有大量的敏感信息，一旦泄露则危害极大。在数据成为企业最宝贵资产的今天，对于数据库中存储的数据安全的保护需求是现代企业信息安全战略的核心组成部分。随着数字化转型的深入，企业越来越依赖于数据库来存储客户信息、交易记录、知识产权、财务数据和运营细节等关键信息。因此，确保数据库数据的安全性对于业务安全变得至关重要，主要体现在以下几个方面：

数据机密性：防止未授权的访问和泄露，确保敏感信息仅对合法用户开放。这包括加密存储和传输中的数据，以及实施严格的访问控制策略。

数据完整性：保证数据的准确性和可靠性，防止数据被非法修改或破坏。通过使用校验和、版本控制和数据审计等机制，确保数据在任何时候都是完整无损的。

数据可用性：确保数据在需要时能够被合法用户及时访问和使用。这要求建立冗余系统、灾难恢复计划和高效的备份策略，以应对各种可能的故障或灾难情况。

审计与监控：持续监控数据库活动，记录所有数据访问和更改，以便于审计和事件响应。这有助于发现潜在的安全威胁和内部不当行为。

身份验证与授权：实施多因素认证和最小权限原则，确保每个用户仅能访问其职责范围内的数据，对于无权限数据要经过脱敏处理，减少内部威胁和误操作的风险。

数据生命周期管理：从数据创建到销毁的整个生命周期内，应用适当的安全措施，包括数据分类分级、归档和安全删除，以保护数据在各个阶段的安全。

满足这些需求需要综合运用技术、政策和人员培训等手段，构建多层次的防御体系，确保数据库数据免受内外部威胁的侵害，为企业运营提供坚实的支撑。

2 产品概览

2.1 产品目标

数达安全公司基于多年数据安全产品研发经验与产品和技术积累，凭借自有研发力量，针对现阶段国内中小型企业数据安全保护市场的需求特征，在原有的多款数据安全专用产品的基础上，研制推出了数安卫士 V5。该系统基于公司传统的数据库资产管理、数据库审计、数据库防火墙、数据库加密、数据库静态脱敏、数据水印、数据库动态脱敏和数据销毁等产品的技术能力，通过能力整合与管控平台的综合管控，实现了对数据库资产的自识别、梳理、监控与防护，实现了全生命周期的数据安全。

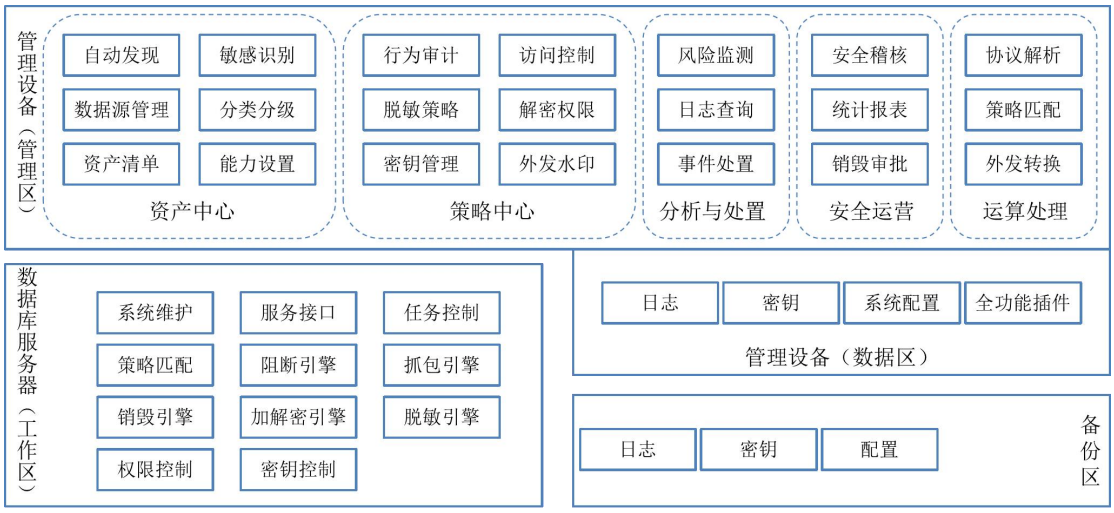
本产品主要实现两个目标：

1）面向中小型组织的所有数据库系统，用单台设备加全功能系统插件的方式满足数据安全防护与合规要求

2）提供数据库资产分类分级、审计、行为阻断、动态脱敏、数据外发水印与脱敏、数据存储加密和数据销毁等全生命周期的全面数据安全防护能力

2.2 产品架构

按照功能的不同，本系统产品结构如下图所示，包括管理区、数据区、工作区和备份区。



管理区和数据区位于数安卫士管理设备中。其中管理区用于实现对整个系统和插件的管理，包括资产中心、策略中心、分析中心、处置中心、安全运营和运算处理等模块。数据区主要用来存储系统的配置、日志、密钥和全功能插件的安装包。

工作区特指工作在数据库服务器上的全功能系统插件，包括阻断引擎、加密引擎、抓包引擎、销毁引擎、脱敏引擎、系统维护、服务接口、权限控制、密钥控制、任务控制和策略匹配等模块。

备份区为独立的容灾模块，用于备份系统的参数、密钥、日志等重要信息，在发生特殊故障的情况下，可以快速恢复系统。

3 产品功能

3.1 资产管理

（1）自动发现资产

根据数据库的通信协议特征自动扫描网络流量，以识别网络中可能存在的各种数据库，即使修改常用端口号也可以发现，免配置一键添加目标数据库，减少数据库配置工作量。

（2）敏感数据发现

自动扫描数据源，依据内置的上百种敏感数据识别规则，对数据源的内部数据进行自动随机抽样、识别解析、发现敏感数据，为数据库数据资产分类分级和安全防护能力设置提供有意义的参考。

（3）资产梳理与分类分级

对自动发现的数据库资产，依据预定义的敏感数据识别规则和数据分类分级标准，对数据库资产的内部数据进行梳理、打标和分级分类，既满足数据分类分级合规要求，又为后续设置数据安全保护能力提供依据和参考。

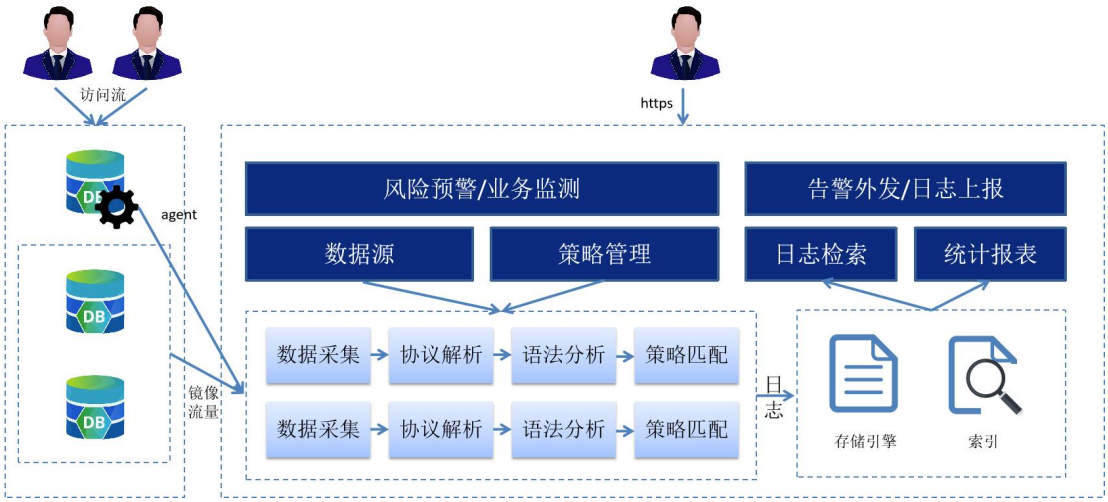
3.2 行为监管

（1）行为监测-数据库审计

行为监测通过监控数据库的多重状态和通信内容，不仅能及时掌握数据库所面临的数据风险访问，而且可以通过完整的访问日志对发生的安全事件进行事后追查。

通过高效的策略引擎能够及时的发现各类针对数据库的越权访问和攻击的行为指纹，采用具有专利技术的并行存储引擎，能够轻松应对高吞吐量的 SQL 日志存储。结合特殊优化的索引技术，快速生成各类协议、访问行为特征的关键字索引。即使对超亿级的审计日志进行的关键字查询时，能够秒级返回查询结果。能够真正帮助用户在面对各类数据库的行为审计时，做到：立即发现、立即告警、立即溯源。

行为监测支持在数据库服务器安装抓包 agent 和镜像流量导入两种获取流量的方式，在数安卫士设备内完成协议解析、策略匹配、生成索引和存储日志等功能。



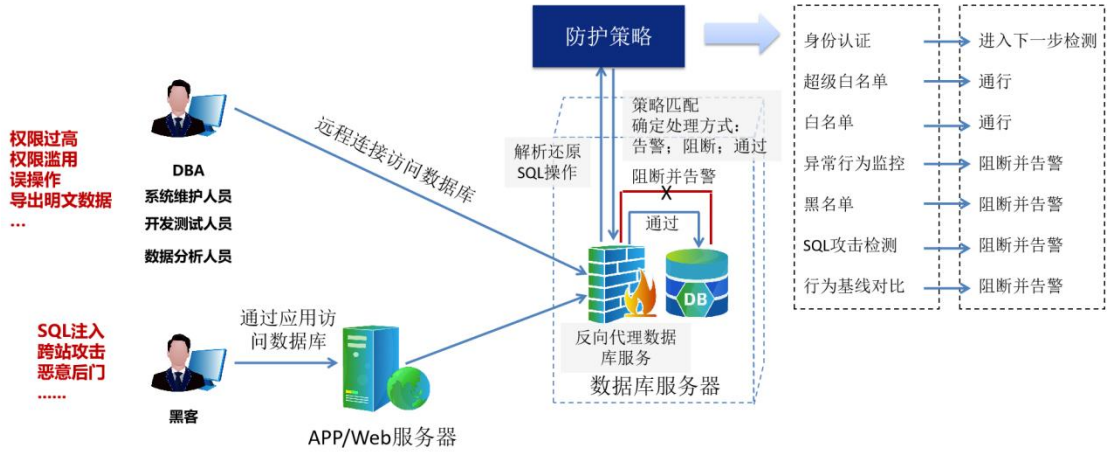
（2）行为管控-行为阻断

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。

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。

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，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。

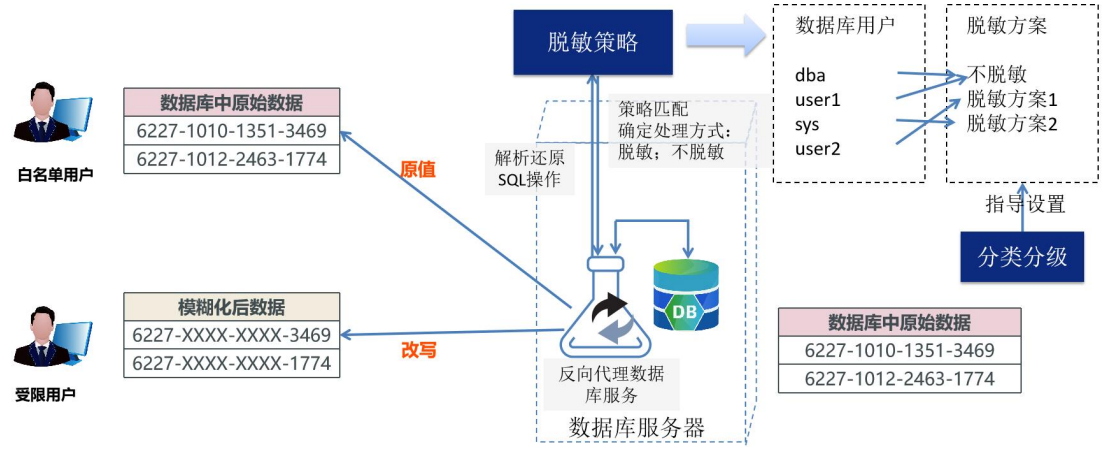
行为管控通过部署在数据库服务器上的行为管控 agent 在本地反向代理数据库访问流量来实现，在数据库服务器本地完成协议解析、策略匹配和会话阻断或告警等功能，该功能会屏蔽直接访问数据库的通道，防止数据库节点被各类攻击者、扫描工具发现，从而诱发的各类攻击行为，保证核心业务安全、平稳地运行。该行为管控 agent 支持软 Bypass 和智能 Bypass 功能，能够保证业务运行不中断，时延低，服务质量有保证，提高系统的高可靠性。



（3）行为管控-动态脱敏

动态脱敏通过截获并修改数据库通讯内容，对数据库中的敏感数据进行在线屏蔽、变形、字符替换、随机替换等处理，达到对用户访问敏感数据真实内容的权限控制。提前可以参考数据分类分级结果设置不同的脱敏方案，并且不同的数据库用户可以在已经设置好的脱敏方案中选择合适的方案，这样对于存储于数据库中的敏感数据，通过脱敏系统，不同权限的用户查询数据时将会得到不同结果展现。

动态脱敏同样通过部署在数据库服务器上的行为管控 agent 在本地反向代理数据库访问流量来实现，当仅设置动态脱敏而不设置行为管控策略时，仅作脱敏判断和操作，不会启动协议解析、策略匹配和会话阻断等功能。仅设置动态脱敏功能时，性能非常卓越，基本可以做到与未设置策略时基本相同的访问时延。



3.3 存储加密

（1）字段加密

可根据实际需求选择对敏感的字段进行加密，敏感字段以密文的方式在硬盘

上保存。即使数据库文件被非法复制或者存储文件丢失，也不会导致真实敏感数据的泄露。

（2）表空间加密

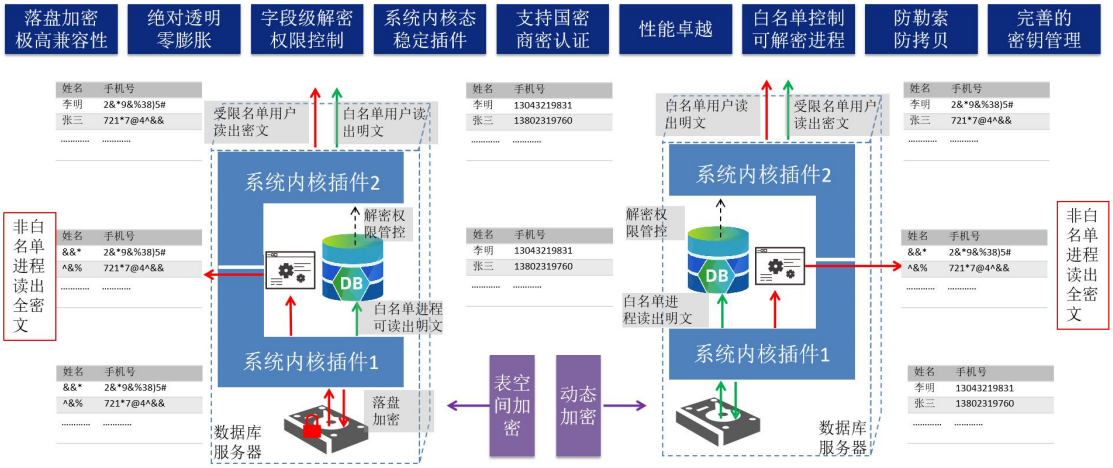
可以选择将敏感字段所在表的表空间文件进行加密，表空间文件以加密方式存储，使得即使数据库本地文件或者存储介质被盗依然能保证数据库内部敏感数据的安全。

（3）动态加密

设置后不会立即将数据加密，而是当数据库文件被读取的时候根据策略有选择性的进行加密，数据库服务进程根据默认策略配置可以读到明文，从而数据库服务可以达到和未实施动态加密前一模一样的性能。而其它文件访问方式读取到

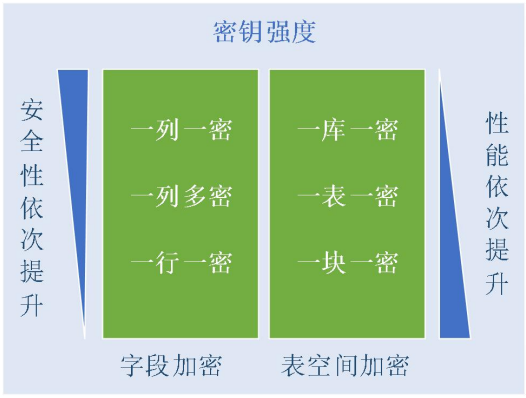
的都是密文。

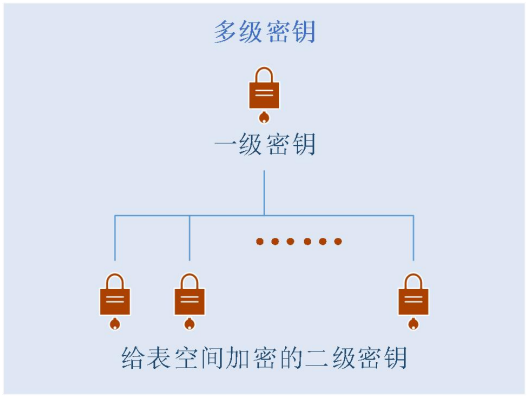
无论字段加密、表空间加密还是动态加密，初始加密过程对数据库用户都是完全透明的，不需要改造应用系统，部署后可立即使用。当完成初始加密后，在数据的使用过程中，新的数据都按照设置即时加密与解密，无需额外二次处理与部署。

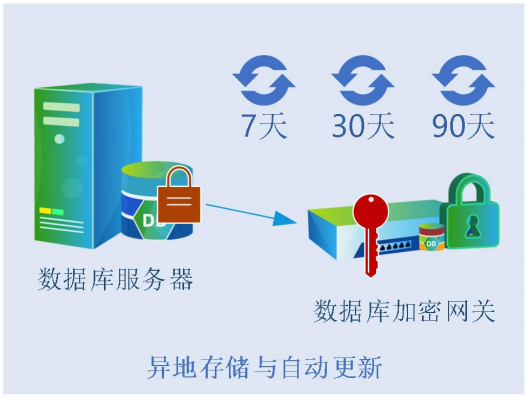


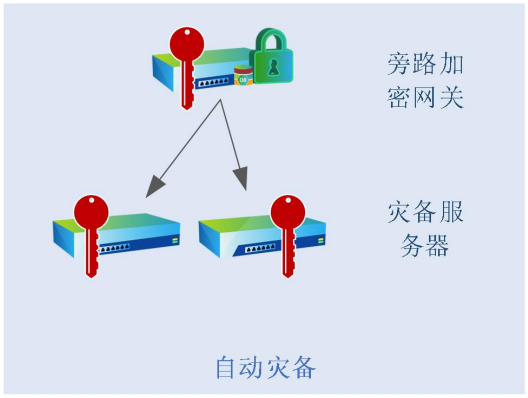
（4）密钥管理

本产品提供了完善的密钥管理和保护机制。采用多级密钥管理方式，所有的工作密钥做二次加密处理；字段加密支持一列一密、一列多密和一行一密三种密钥强度等级，表空间加密支持一库一密、一表一密和一块一密三种密钥强度等级，在这些不同的强度等级下，安全性依次得到提升，性能相应下降，用户可以根据系统实际情况酌情配置；密钥异地生成并保存在加密机上，在数据库本地不保存，以防止数据库服务器硬盘丢失连同密钥一起丢失的风险；可在产品中设置多个密钥灾备服务器并自动备份密钥，以确保密钥的安全可靠存储。可设置按周（7 天）、按月（30 天）或按季度（90 天）自动更新密钥，确保密钥的安全性。



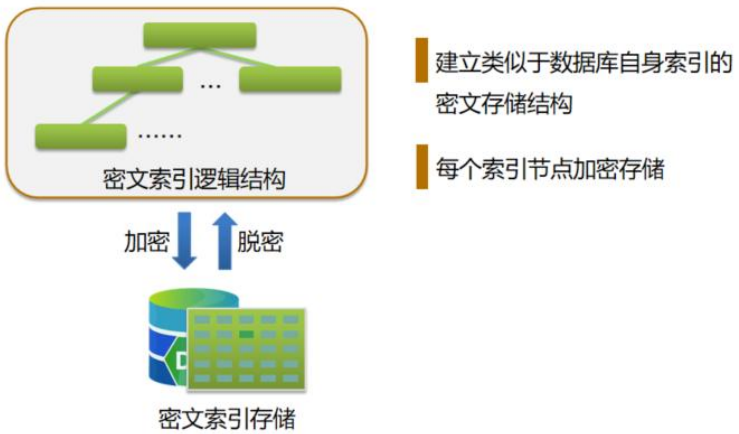






（5）密文索引

当采用字段型加密时，系统提供专利的密文索引技术，借助数据库自身的索引机制为密文建立起索引结构。密文索引避免了操作数据时的全表解密，把敏感字段的加密对数据库访问性能造成的损失降到和加密前没有明显区别。

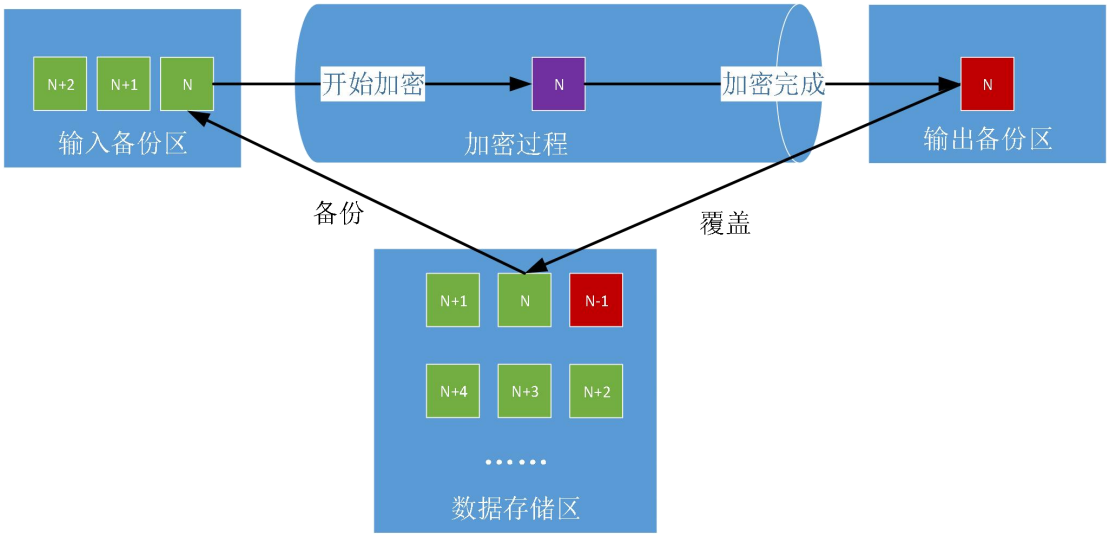


（6）完善的任务管理与过程数据保护

系统提供完善的加解密任务管理机制，可以使得用户对整个加解密任务做到高效管理与有效控制。在加解密发生异常中断后，可以重新启动任务以重试，也

可以建立反向任务，实现可逆操作。

在加解密过程中，对每一个加解密的数据块单元，均在加解密完成前作备份保护处理，以确保在加解密任务执行发生意外时，数据可以回滚，从而保障原始数据的绝对安全。

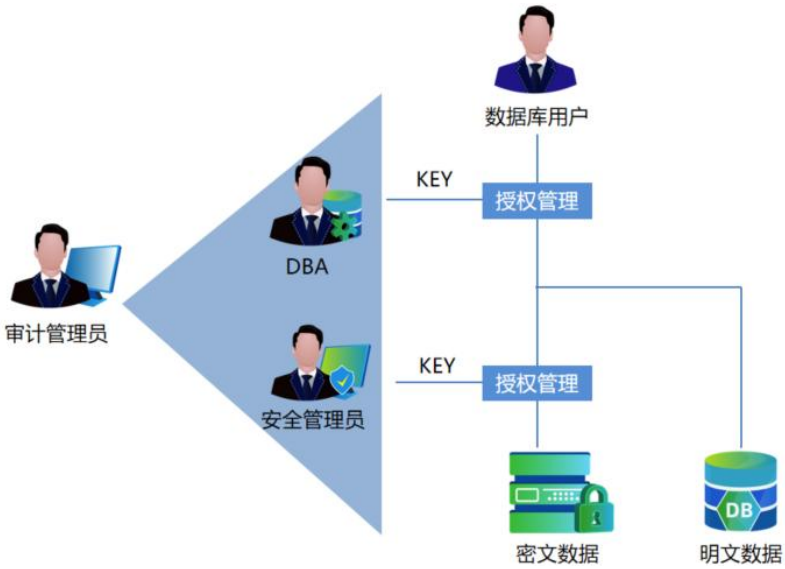


（7）完整性保护

对于加密的字段或表空间支持开启完整性保护功能，可以选择SM4-CBC-HMAC、SM3-HMAC 或 SM3 等算法针对加密字段添加专用校验位用于完整性保护校验。

（8）解密权限管理

对于加密后的敏感数据，系统提供独立的加密解密的权限管理，只有同时经过数据库自身和加密系统联合授权的用户才能对敏感数据进行解密和查看，从而降低数据库超级管理员权限过高造成的泄密风险。数据库加密系统通过内置的安全管理员来设置用户对加密数据的访问权限。

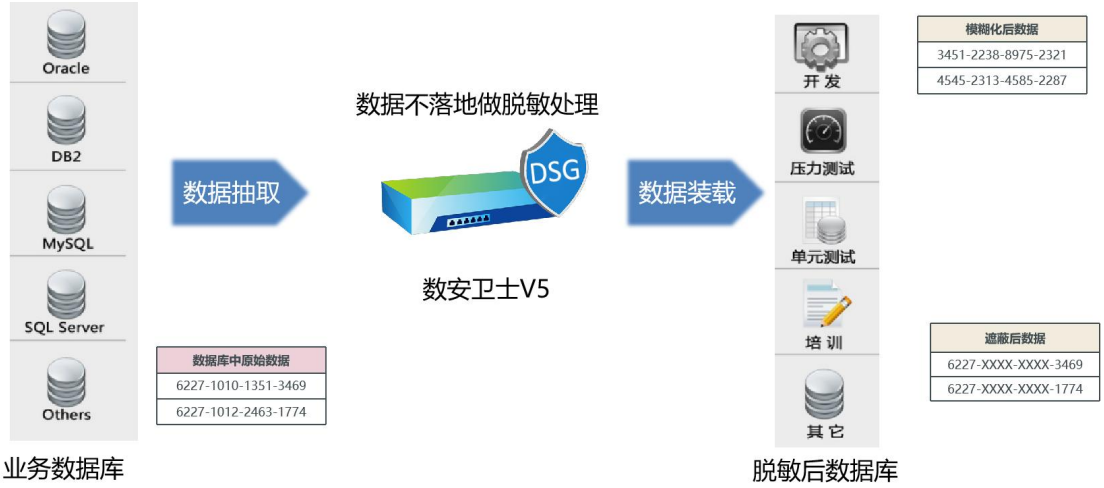


对于字段加密，支持联合应用程序名、客户端 IP、客户端主机名、客户端操

作系统用户名和数据库用户名等共同建立的访问权限策略，能够提供更加细致的权限管理。

3.4 外发安全

（1）静态脱敏



如上图所示，静态脱敏从左到右为脱敏数据的处理流程。主要是将生产环境中的数据抽取到脱敏系统的内存中，不落地的通过算法识别并脱敏后，高效的写入开发、测试以及大数据分析平台的数据库中。

静态脱敏支持用户自定义不同范围的脱敏方案。能够对需要脱敏的数据范围进行自由选择，提供库级、表级、列级、行级的多种层次的范围设置。还提供 where 条件对原始的数据进行过滤，比如只需要一张表中的几个数据字段和部分数据量时，只需要简单设置即可。

在单个表的字段进行组合查询后的数据脱敏的基础上，提供了数据子集配置，通过表与表之间的主外键关联关系，能够对多个表的任意列进行组合脱敏。满足用户不同场景下的脱敏需求。

同时提供了增量脱敏配置，为了满足持续增长的业务数据脱敏需要，通过对敏感表的增量脱敏条件进行配置，帮助用户保持测试库环境与生产库环境的数据总量一致。

静态脱敏支持库到库、库到文件、文件到库和文件到文件四种脱敏方式。

（2）数据水印

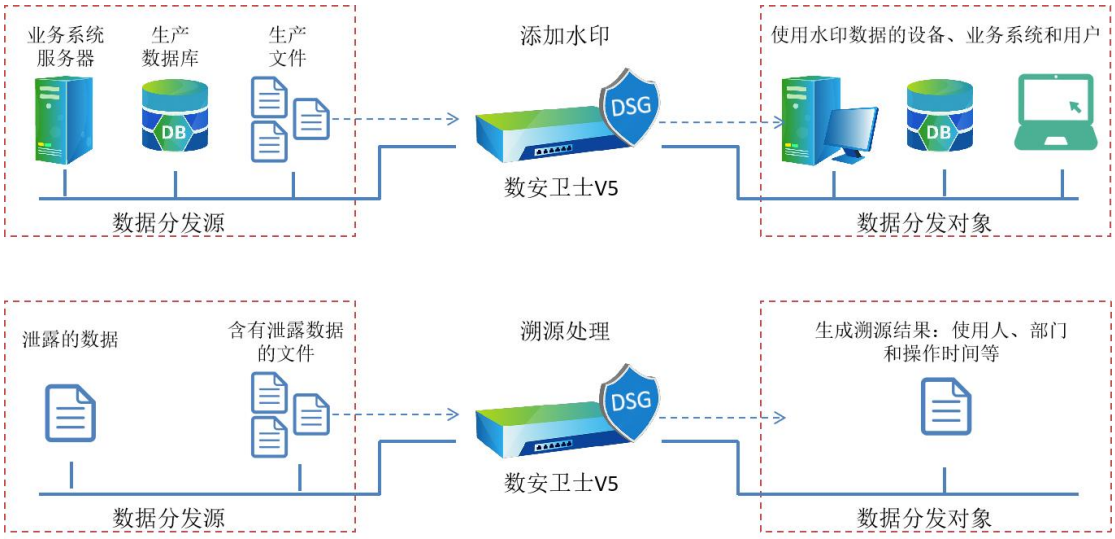
数据水印功能可以对外发的数据增加水印标记，装载至目标数据库或者文件服务器中，为隐私数据的共享提供双重的保险机制。

当出现数据泄露时，可以通过多种途径对已泄露的数据进行精准溯源，找到泄漏数据的使用人身份、部门以及操作时间等信息，快速关联到脱敏任务，确认已泄漏的数据范围和途径。溯源方式主要包括：文本溯源和文件溯源两种方式。

数据水印具有以下特点：

- 对所有的字符型数据采用任意位置的方式插入水印标记；
- 水印标记和使用人进行唯一性关联，详细记录使用人的姓名、部门信息；
- 水印锁定，当水印标记被使用后，自动锁定，防止篡改；
- 精准溯源，采用全文检索的方式查找水印标记，并自动显示水印标记数量、使用人信息；
- 多种溯源方式，复制粘贴、上传文件均可。

通过建立水印和数据使用者的对应关系，能够帮助用户对泄漏的数据进行快速溯源，及时追踪到泄漏数据的第一责任人和部门信息，以便追责。



3.5 数据销毁

数据销毁是数达安全基于对数据库、操作系统内核、存储文件结构和磁盘安全技术的深入研究与分析，开发了基于数据库敏感数据识别算法、多种多次彻底的磁盘覆盖算法和操作系统内核级的销毁引擎，使得在高效发现数据库敏感数据所在文件的基础上，采用有效覆盖算法从操作系统内核对磁盘进行彻底的擦除，消除任何通过技术手段恢复数据的可能。

表空间的销毁采用基于操作系统内核扩展的方案，在对数据库存储文件结构的精确的理解的基础上，通过操作系统提供的文件驱动及 HOOK 机理，实现表空间文件落盘存储区域的精准捕捉与销毁。通过对文件原位的精准捕捉与多次写入来确保原始数据的彻底销毁。并在该技术的基础上，还可以扩展到对操作系统某个具体文件、空闲磁盘和全盘的擦除。

销毁功能由销毁引擎远程实现，可以将销毁引擎远程安装在目标服务器上，销毁设备实现远程管理。

表空间销毁是对数据库表空间文件调用覆盖算法反复写入，精准擦除表空间

文件所在磁盘区域，不影响系统和数据库运行。对于重要文件也可以采用相同原理做专门性的擦除，建议配合空闲磁盘擦除一同使用，确保磁盘上没有任何该文件的残留。这两种方式本质上都是精准销毁未释放的磁盘空间。

空闲磁盘擦除是针对磁盘的空闲未用空间做全面擦除，确保已经删除的文件被彻底销毁，无法恢复。全盘擦除可以针对本地或远程挂载的整块非系统磁盘作全面擦除，确保彻底销毁磁盘上原有数据，便于后期二次重复利用。

支持 DOD 5220.22-M、DOD 5220.22-ECE、VSITR 和 Gutmann 等多种专业软销毁算法，确保安全高效实现数据的彻底销毁。

3.6 系统安全

（1）双机热备

加密引擎可以同时与两个旁路加密管理机通信，数据源引擎、参数配置与密钥均可以同步互备，确保一个系统出现故障时不影响数据块加密引擎的正常使用，确保整体系统的高可用性。

（2）三权分立

根据等级保护等相关评测要求，系统设置安全员、审计员、系统管理员三种角色。安全员负责设置和执行加密策略，加密参数等；系统管理员负责设置系统自身设置，比如系统端口设置、系统时间等；审计员对包括安全员、系统管理员在内的所有角色的行为进行审计。

（3）双因子认证

为避免基于账号、口令的单一认证方式安全性较低的问题，本系统实现了基于账号、手机应用程序和基于时间的动态码的多种要素的身份认证。

（4）国密登录方式

针对不同的用户，支持采用国密算法的智能密码钥匙方式登录。

（5）基于 GMSSL 的加密通信

数据库服务器与设备间的通信采用 GMSSL 加密方式，确保通信安全。

4 特性与优势

4.1 全面的高度集成的安全防护能力

整合自多年全部自研的核心技术积累，全面覆盖各项数据安全能力要求，分类分级、审计、阻断、动脱、静脱、水印、加密和销毁等。

4.2 高可靠性

- 高可靠的工控设备，支持双机热备，确保运行可靠；
- 完善的密钥管理和备份机制，确保加密数据可以可靠的解密；
- 10+年以上成熟技术与产品整合，产品使用稳定可靠。

4.3 易用性

- 对应用程序访问过程完全透明的系统内核插件，无需客户端做任何改动，最小化对其它系统的影响；
- 提供基于浏览器的简单、友好、便捷的统一管控中心，支持多用户并发访问，支持数据的同步，支持事务机制；
- 仅需旁路部署设备和分布式部署系统探针，集中式统一管理。

4.4 强大的兼容性

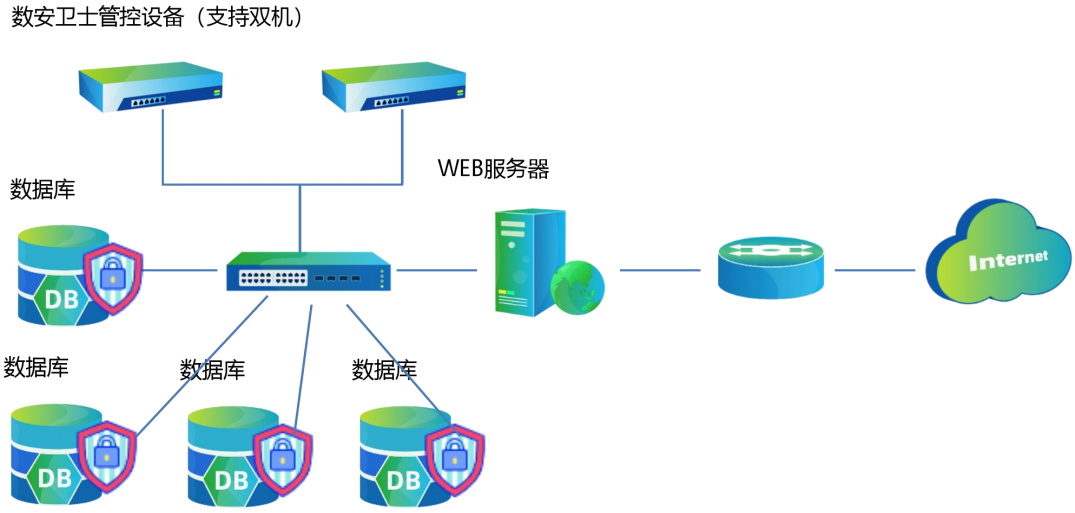
产品具有良好的兼容性，支持国内市场上主流的操作系统和数据库系统。

产品支持的操作系统：WINDOW/LINUX/UNIX；

支持几乎所有的传统数据库、国产数据库和大数据环境：包括 Oracle、Db2、SQL Server、GBASE 8a/8t/8s、Hive、MySQL、达梦、Treadata、PostgreSQL、Greenplum、Sybase、Cache、Informix、MariaDB、Hbase、mongoDB、人大金仓、神州通用、星环 tdh、Redis、Impala 和 TiDB 等。

5 典型部署

数安卫士部署简单，旁路部署，只要与被保护的目标数据库服务器路由可达即可。在数据库服务器上根据需要安装全功能系统插件，实现各项保护能力。



6 产品规格

型号	硬件配置
DS-DSG-1000	1U，6 千兆电，单电源，i3，2TB 硬盘，16G 内存； 数据库规模：千万级记录； 支持数据库数量：默认 1 个；最多 5 个 支持功能：自动发现数据源、敏感数据识别、资产分类分级、行为审计、行为阻断、动态脱敏、存储加密、静态脱敏、数据水印、数据销毁。
DS-DSG-3000	2U，6 千兆电，冗余电源，E3，2TB 硬盘，16G 内存，可扩展 X8 加密卡； 数据库规模：千万级记录； 支持数据库数量：默认 5 个，最多 30 个； 支持功能：自动发现数据源、敏感数据识别、资产分类分级、行为审计、行为阻断、动态脱敏、存储加密、静态脱敏、数据水印、数据销毁。
DS-DSG-5000	2U，6 千兆电，冗余电源，E5，2TB 硬盘，16G 内存，可扩展 X16 加密卡； 数据库规模：亿级记录； 支持数据库数量：默认 30 个，最多 50 个； 支持功能：自动发现数据源、敏感数据识别、资产分类分级、行为审计、行为阻断、动态脱敏、存储加密、静态脱敏、数据水印、数据销毁。

7 产品价值

7.1 全面提升中小企业数据安全治理能力

数安卫士是综合考量数据体量与访问流量，为中小企业数据安全量身打造的全面的高度集成的数据安全解决方案。数据库到应用系统这一段是信息安全的最后一公里，也是最后一道防线，涉及的是最直接的敏感数据安全管理，直接关系到敏感数据的安全。数安卫士系统通过全面的数据安全能力保护，增强了数据库的安全性，完善了数据的纵深防御体系，提升了整体安全治理能力。

7.2 帮助中小企业降低数据安全合规成本

通过部署数安卫士，可以轻松满足密评、等保、网安法、数安法、关键基础设施保护条例等国家级法律法规要求，也可以轻松满足教育行业、医疗卫生行业、政府行业等各种行业数据安全要求。同时提供了采购多款昂贵的单能力数据安全合规产品的替代解决方案，降低总体合规成本，提升了企业的经济效益。

7.3 为数据库分布模式为多、小、散的组织提供可行的数据安全治理解决方案

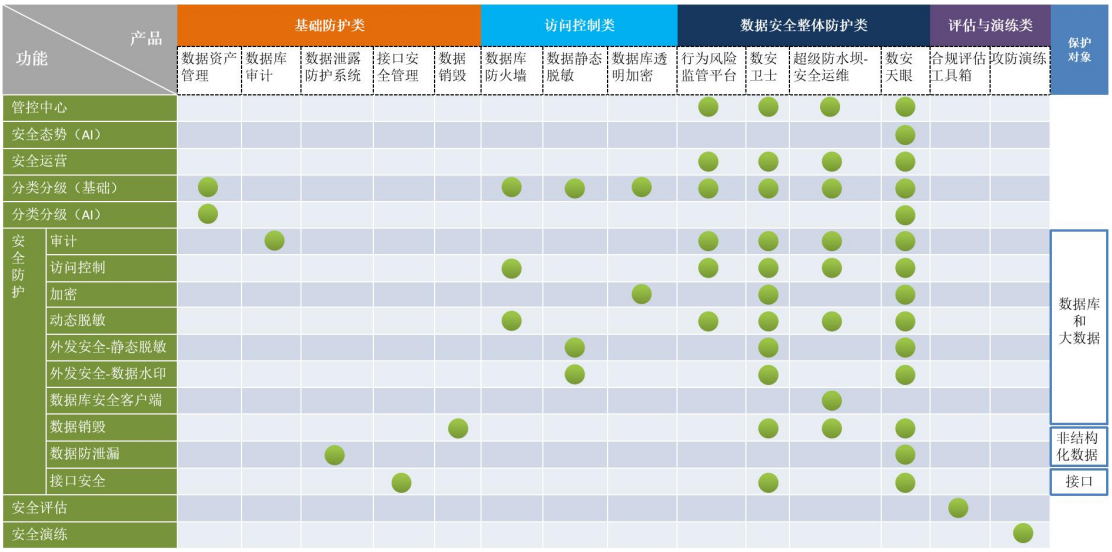
当数据库分布模型为多、小、散的形态时，数据库数据资产的部署和管理都相对困难，传统单能力的旁路或网关式的数据安全产品也很难用少量低成本设备覆盖所有资产。数安卫士通过给所有数据库系统部署全功能系统插件和单设备集中管控的方式，很好的解决了此种情况下的数据安全管控难题。

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全国二十多个省设置了办事处，服务全国客户。