RELIABLE NETWORK
SAFE WORLD
TOPSEC

天融信昆仑系列数据库审计系统

技术白皮书

北京市海淀区西北旺东路 10 号院西区 11 号楼 1 层 101　天融信科技集团

100193

电话：010-82776666

传真：010-82776677

服务热线：4007770777

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

变更记录

版本	修订日期	修订人	修订类型	修订章节	修订内容
V23.1.0	2023/5/5	莫雪骄	A	ALL	ALL
V23.1.1	2024/2/22	龚启光	A	ALL	ALL

*修订类型分为 A- ADDED M- MODIFIED D -DELETED

注：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目录

1 产品概述 1

1.1 背景介绍 1

1.2 系统架构 1

2 产品特点 3

2.1 数据库类型审得全 3

2.2 数据库资产可视化 3

2.3 即查即统高效查询 4

2.4 审计要素精准详实 4

2.5 满足用户合规需求 5

3 产品功能 6

3.1 全面数据库审计 6

3.2 清晰的资产监控 6

3.3 细粒度操作还原 7

3.4 精准的业务关联 8

3.5 智能的行为基线 9

3.6 数据库性能分析 9

3.7 数据库威胁检测 10

3.8 精细的业务报表 11

3.9 云环境审计支持 11

3.10 全场景协同联动 12

3.11 可靠的系统管理 13

3.12 灵活的双协议栈 13

3.13 高效的数据脱敏 13

4 部署模式 15

4. 1 旁路部署 15

4. 2 级联部署 15

4.3 分布式部署 16

5 产品规格 17

6 产品资质 18

1 产品概述

1.1 背景介绍

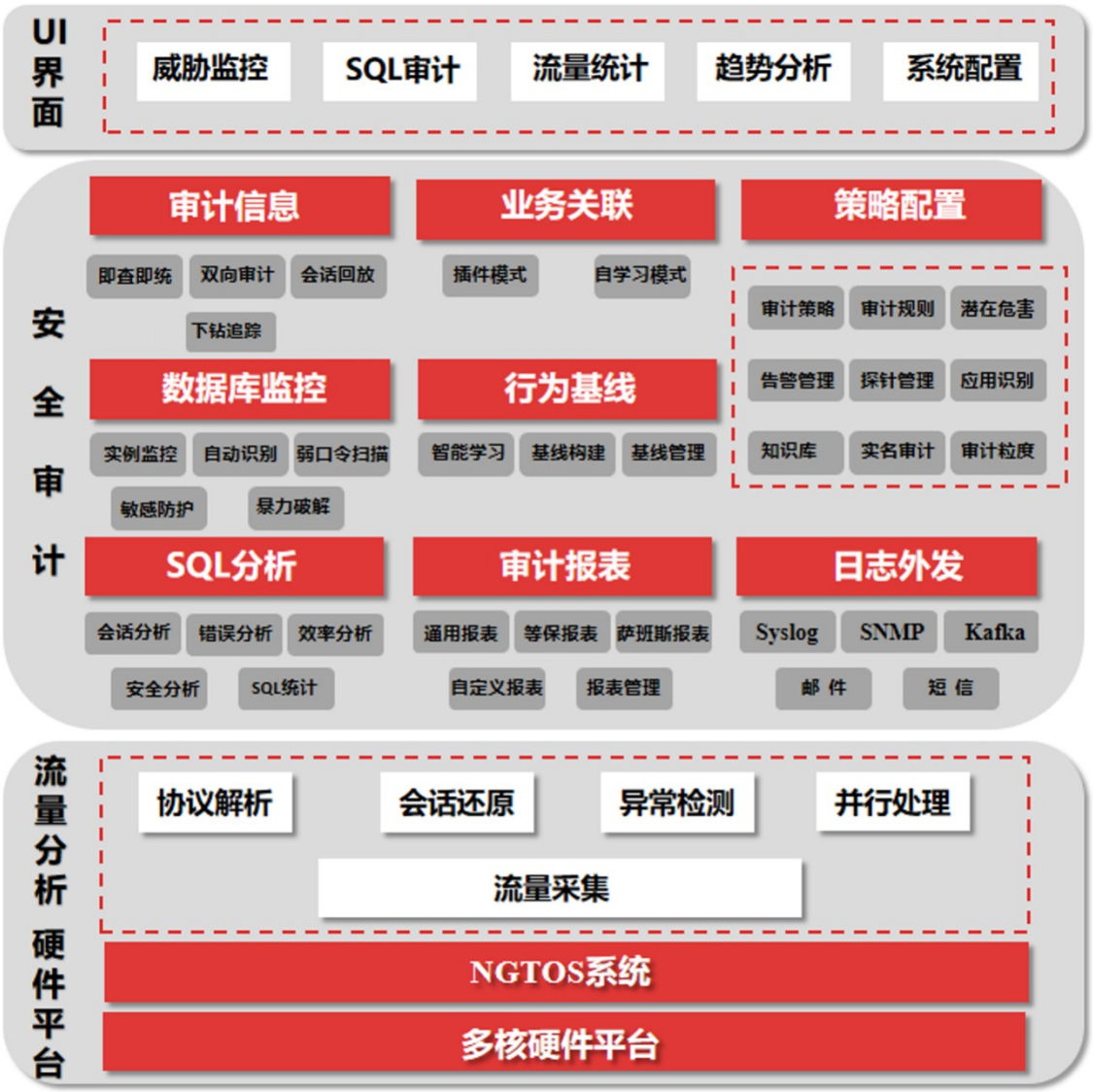
随着 IT 技术的飞速发展，数据库已经成为信息技术的重要组成部分，是现代计算机信息系统和计算机应用系统的基础和核心。数据库作为商业公司中最具有价值的重要资产，通常都保存着重要的数据信息，这些信息资产面临的挑战日趋严峻。据《2018 数据泄露损失研究》评估显示，大型数据泄露代价高昂，百万条记录可致损失 4000 万美元，5000 万条记录可致损失 3.5 亿美元。遭遇数据泄露事件的公司企业平均要损失 386 万美元，同比去年增加了 6.4%。数据库泄漏防不胜防，主要是部分企业单位安全意识薄弱，未采取相应的技术手段，还在采用数据库本身日志文件实现审计，该方式的缺点是：会影响数据库本身性能、数据库日志文件易篡改、操作日志查看不直观。

另外，GB/T22239-2019《信息安全技术网络安全等级保护基本要求》也对安全审计也提出了明确要求，在国家法律法规层面确定了安全审计的重要性；还有强调 IT 系统内部控制的《萨班斯法案》与《银行业金融机构信息系统风险管理指引》等。

针对以上需求场景，传统的安全设备难以胜任，需要专业的数据库审计系统记录用户对数据库的操作行为。天融信数据库审计系统（以下简称“TA-DB”）是一款针对上述环境推出的专业数据库审计产品，该产品提供数据库实时监控、数据库风险预警、数据库威胁阻断等功能，充分满足政府、金融、公安、能源、运营商、教育、军工、交通、企业等各行各业的数据库审计需求。

1.2 系统架构

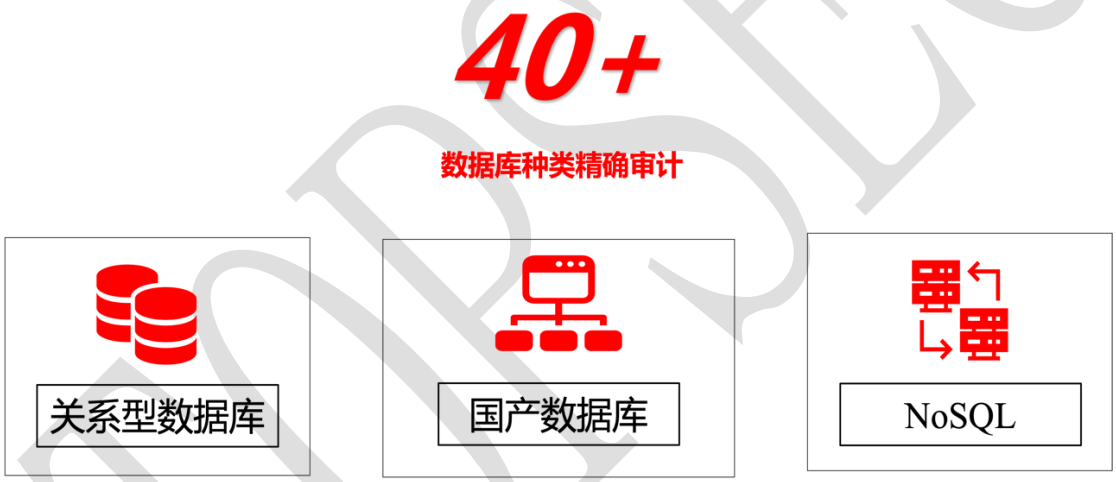
天融信昆仑系列数据库审计系统（TA-DB）基于飞腾 CPU 和麒麟操作系统，采用全模块化设计、中间层理念，形成了先进的多核架构技术体系，从而保证在国产硬件平台上的 TA-DB 产品具有高速的数据审计解析能力，能够胜任复杂网络环境下的安全审计要求。系统架构如下图：


UI界面
威胁监控
SQL审计
流量统计
趋势分析
系统配置
安全审计
审计信息
即查即统
双向审计
会话回放
下钻追踪
业务关联
插件模式
自学习模式
策略配置
审计策略
审计规则
潜在危害
告警管理
探针管理
应用识别
知识库
实名审计
审计粒度
数据库监控
实例监控
自动识别
弱口令扫描
敏感防护
暴力破解
行为基线
智能学习
基线构建
基线管理
SQL分析
会话分析
错误分析
效率分析
安全分析
SQL统计
审计报表
通用报表
等保报表
萨班斯报表
自定义报表
报表管理
日志外发
Syslog
SNMP
Kafka
邮 件
短 信
流量分析硬件平台
协议解析
会话还原
异常检测
并行处理
流量采集
NGTOS系统
多核硬件平台

2 产品特点

2.1 数据库类型审得全

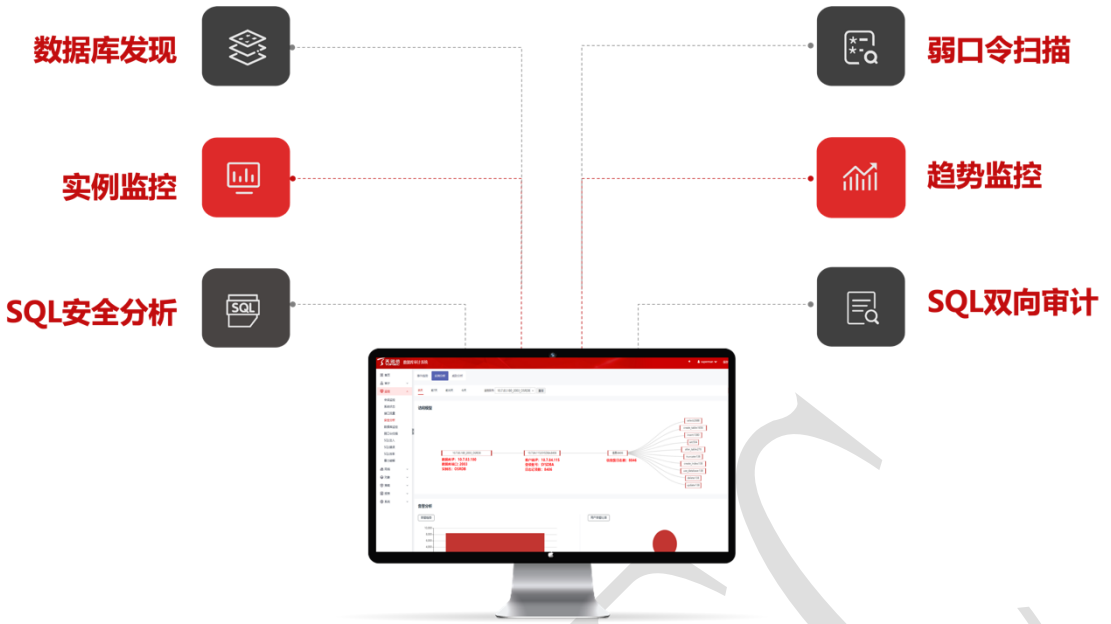
TA-DB 产品利用协议解析技术准确识别数据库类型，能够精准识别并审计主流数据库、关系型数据库、国产化数据库、NoSQL 等 40 多种数据库协议类型，支持数据库协议类型业界领先。包括但不限于：Oracle 系列、SQL Server 系列、GreenPlum 系列、mongoDB 系列、MYSQL 系列、PostgreSQL 系列、Cache 系列、达梦系列、TDSQL 系列、GoldenDB 系列、GaussDB 系列、人大金仓系列、南大通用系列。



2.2 数据库资产可视化

TA-DB 将审计到的 SQL 语句与资产实例结合，内置的数据轨迹模型，以资产为核心，以数据流转为轨迹，图形化展示操作行为，让数据轨迹清晰可见。TA-DB 根据审计到的 SQL 数据，实时发现活跃实例，发现未知的、潜在危害的实例。实时感知资产健康状况，并可根据安全模型对其进行安全风险评估。

TA-DB 的数据轨迹模型，以资产为核心，以数据流转为轨迹，有效解决实例难发现、资产难管控、风险难评估的问题，实现了数据轨迹清晰可见。



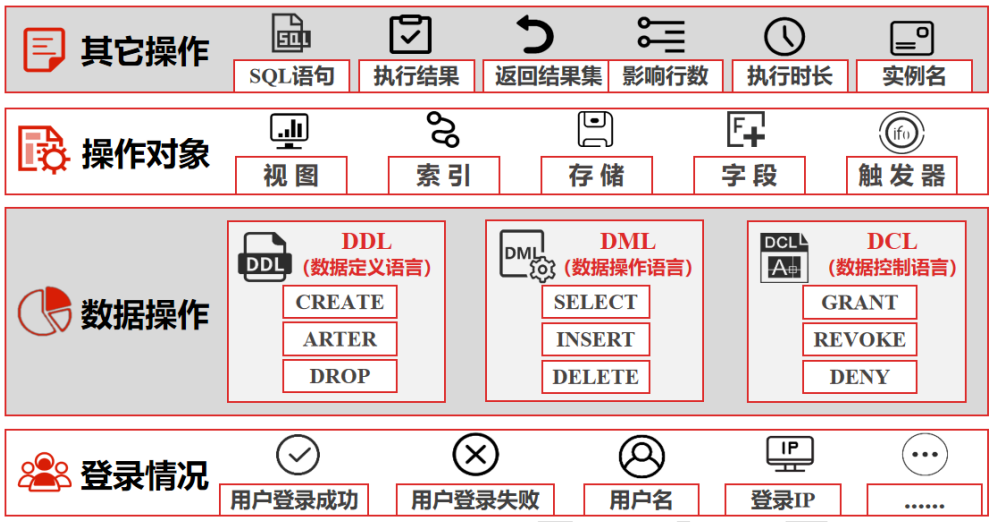
2.3 即查即统高效查询

TA-DB 产品基于自研高效检索算法，优化底层数据结构，并结合前端页面异步加载技术，可实现多维度自定义查询，即查即统，查询结果在前端页面快速呈现，最终可实现千万级数据秒级回显。

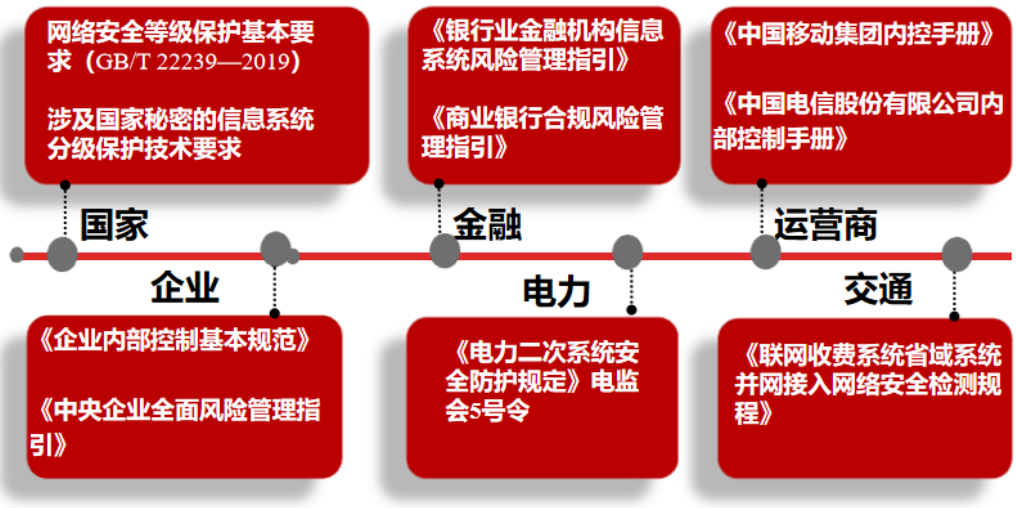
2.4 审计要素精准详实

TA-DB 可对网络流量进行高速、精准解析和还原，不仅可以实时审计各种数据库操作（DDL、DML、DCL 等），还可以审计和还原数据库返回结果，返回的结果涵盖源目的 IP、数据库用户名、SQL 语句、SQL 返回结果集等字段内容。

TA-DB 将数据库的所有访问情况实时可视化展示，管理者可快速回溯定责各种数据库安全事件，有效加强内部审计监督能力。



2.5 满足用户合规需求



通过使用 TA-DB 可有效帮助网络运营者满足等保 2.0 中安全审计、《萨班斯法案》与《银行业金融机构信息系统风险管理指引》中安全审计的相关要求，进而全面提升网络运营者的网络安全防护能力，保障网络的稳定运行。

3 产品功能

天融信数据库 TA-DB 主要的功能模块包括清晰的资产监控、细粒度的操作还原、精准的业务审计等 12 个部分。

3.1 全面数据库审计

TA-DB 通过数据库协议自动识别技术，结合灵活的审计策略，可对国际、国内、NoSQL 等 40 多种数据库在进行全面审计，包括但不限于 Oracle 系列、SQL Server 系列、GreenPlum 系列、mongoDB 系列、MYSQL 系列、PostgreSQL 系列、Cache 系列、达梦系列、TDSQL 系列、GoldenDB 系列、GaussDB 系列、人大金仓系列、南大通用系列：

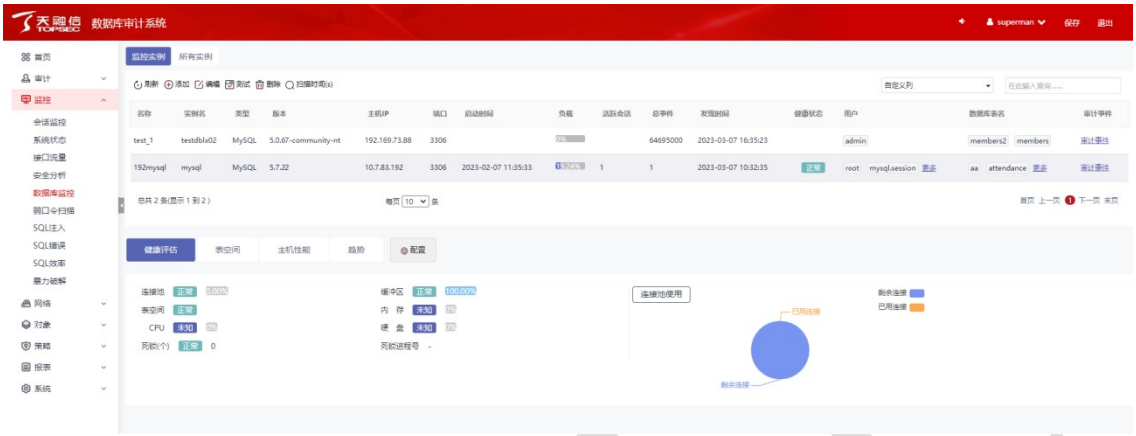
3.2 清晰的资产监控

TA-DB 内置的数据轨迹模型，以资产为核心，以数据流转为轨迹，图形化展示操作行为，让数据轨迹清晰可见。通过实例发现，让隐藏在网络环境中的已知数据库实例、未知数据库实例、潜在风险数据库实例清晰可见。

将核心实例所属资产加入监控，除监控资产的基本信息外，诸如内存、硬盘、CPU，还可深入实时监控资产负载、活跃会话、总会话、连接池、表空间、缓冲区、事务数、游标、用户数、进程死锁等信息。TA-DB 还支持基于实例的审计事件、告警事件等进行会话趋势、

事件趋势、告警趋势、访问源趋势的分析，并综合评估资产的健康状况，保证资产的可用性和响应能力。

TA-DB 还内置上亿条弱口令样本库，采用无损伤破解技术，完成对资产弱口令的检测。



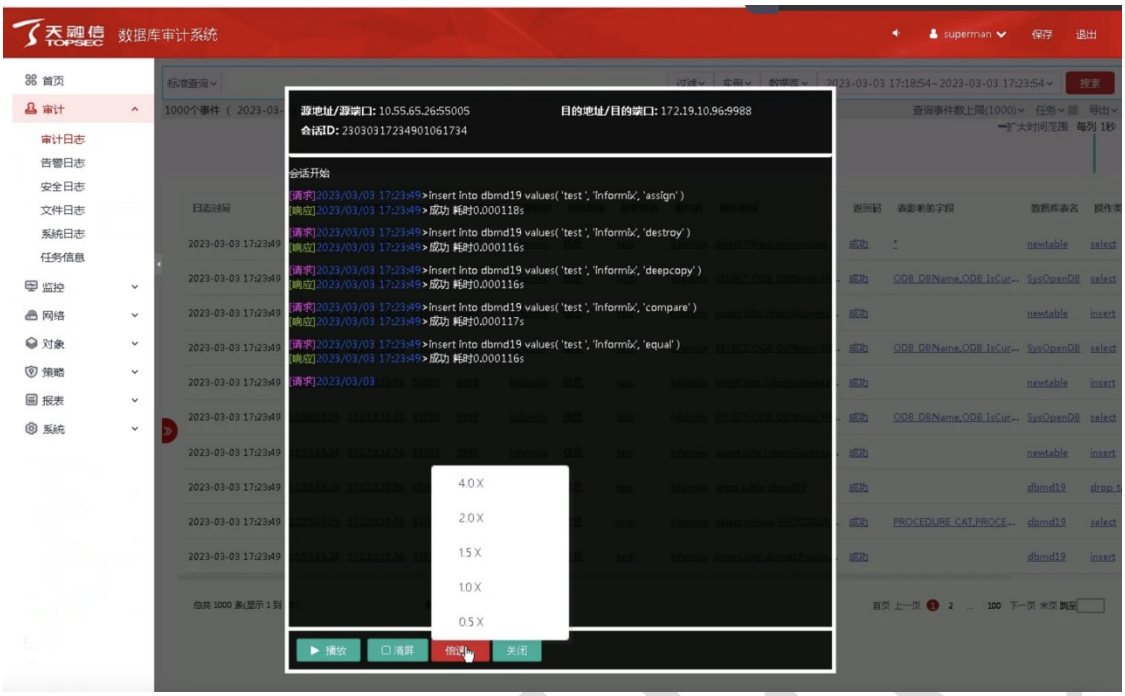
3.3 细粒度操作还原

TA-DB 通过对双向数据报文的识别、解析，不仅解析出基本的五元组信息、基本的数据库协议要素，还可根据业务要求进行更细粒度的 SQL 解析。

TA-DB 支持全类型的绑定变量解析和全类型的结果集解析，内置完备的知识库，可将 SQL 错误码翻译成 SQL 错误信息，并提供数据库原厂商问题解决方案。

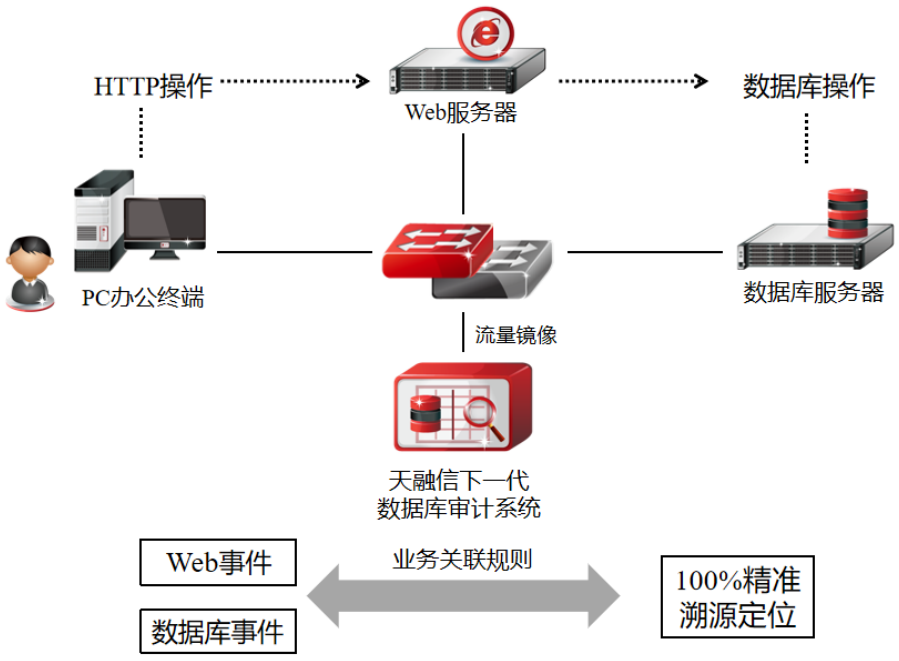
TA-DB 支持超长 SQL 语句解析，保证 SQL 语句零遗漏的审计；此外，友好的界面可实现审计结果详情完整展示、SQL 会话倍速回放等。

细粒度的操作还原为安全分析与业务关联提供夯实的数据基础。



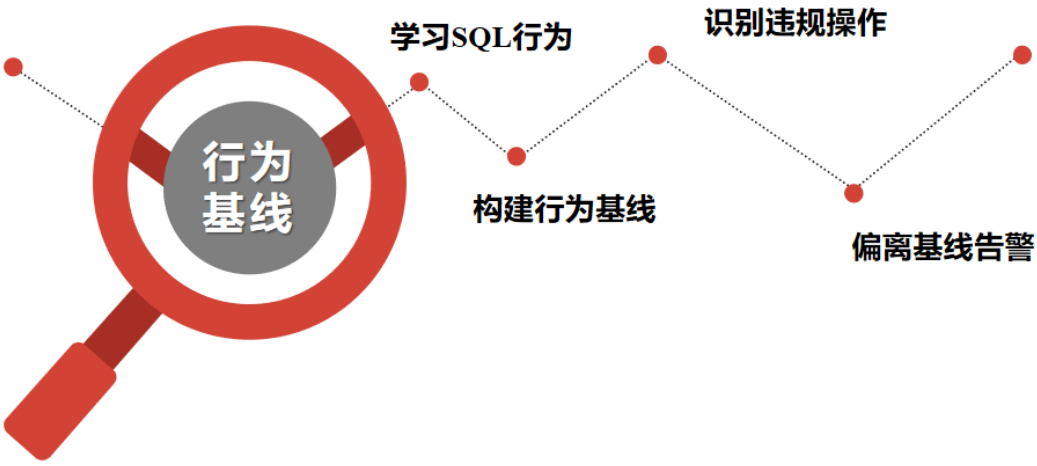
3.4 精准的业务关联

通过对浏览器与 Web 服务器、Web 服务器与数据库服务器之间所产生的 HTTP 事件、SQL 事件进行业务关联分析，管理者可以快速、方便的查询到某个数据库访问是由哪个 HTTP 访问触发，定位追查到真正的访问者，从而将访问 Web 的资源账号和相关的数据库操作关联起来，100%精准展示终端用户对数据库的操作行为。



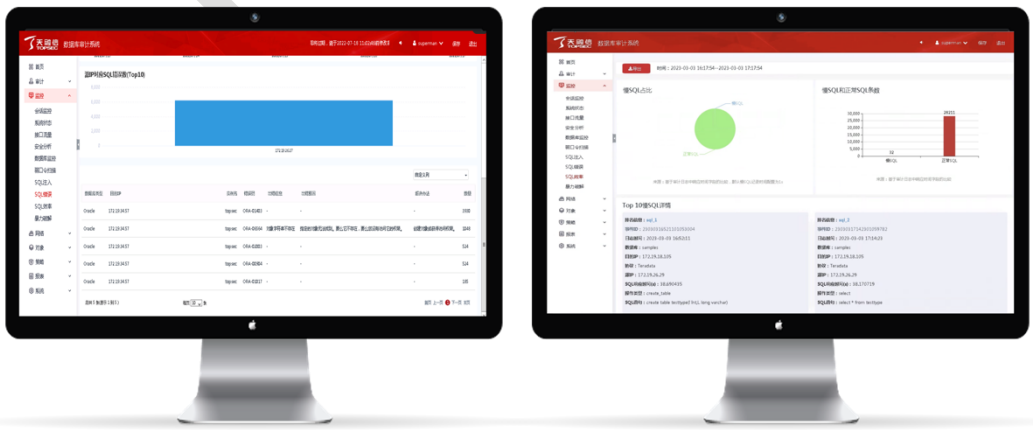
3.5 智能的行为基线

TA-DB 内置强大的智能学习算法，可基于一定业务周期内的审计数据进行学习，生成行为基线，基于此行为基线，对后续的 SQL 事件进行检测，对于偏离基线的行为产生异常告警。



3.6 数据库性能分析

TA-DB 内置性能分析引擎，可对 SQL 执行效率进行分析，可发现内部数据库的性能薄弱处、动态呈现内部资产存在的异常情况，帮助用户及时发现内网数据库性能隐患。同时，系统能够多维度展示用户 SQL 操作错误的占比及趋势，从源 IP 维度以柱状图展示 SQL 错误数，以列表形式给出出错原因、出错信息以及解决办法。

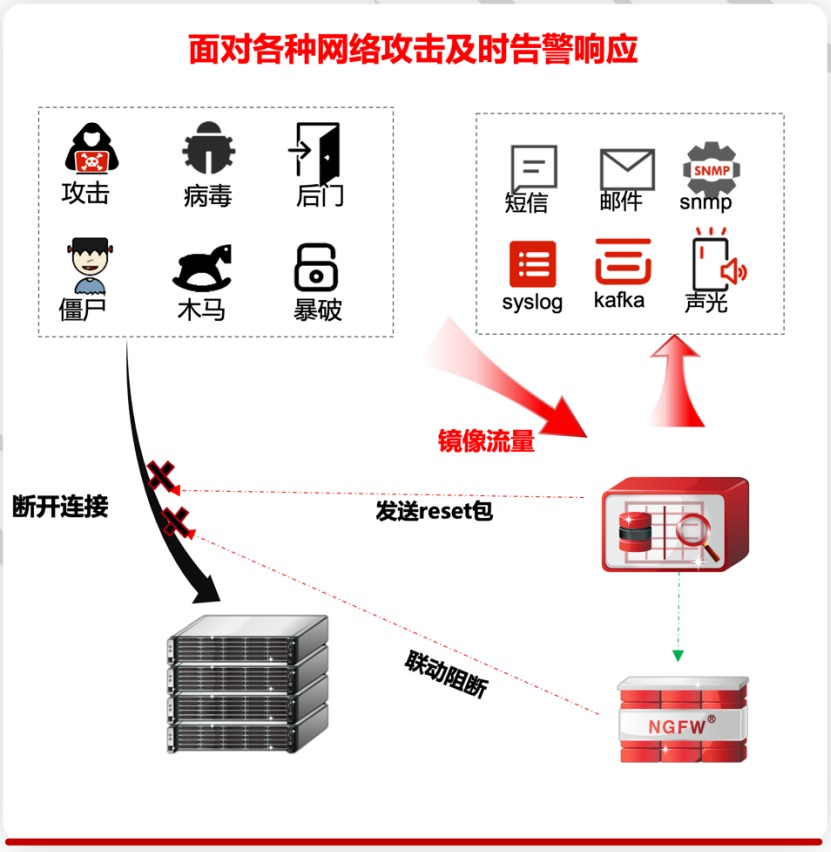


3.7 数据库威胁检测

TA-DB 内置强大的攻击检测引擎，可高效实现漏洞检测、僵尸主机检测，可对 SQL 注入、XSS 跨站攻击、缓冲区溢出、拒绝服务攻击等危险行为实时告警。

除内置的权限管控策略外，TA-DB 还可针对登录用户、SQL 语句、操作类型、操作对象等所有数据库协议要素配置全方位的告警策略，判断事件的危险级别，进行实时的响应处理。

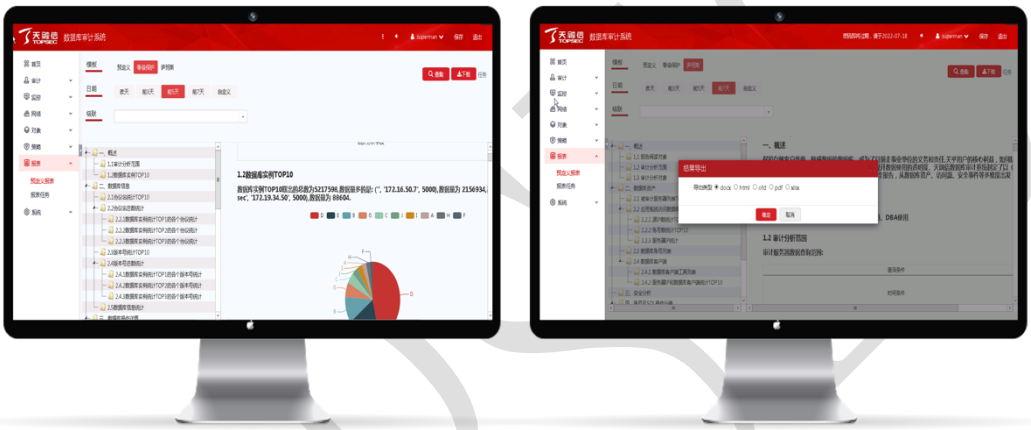
对于需要对一定连续时间内的连续事件进行综合分析才能发现的潜在危险行为，TA-DB 提供了强大的潜在危害分析和关联分析引擎，可以有效检测潜在的危险行为，同时还支持用户自定义攻击检测行为模式，配置更加灵活的检测策略。



3.8 精细的业务报表

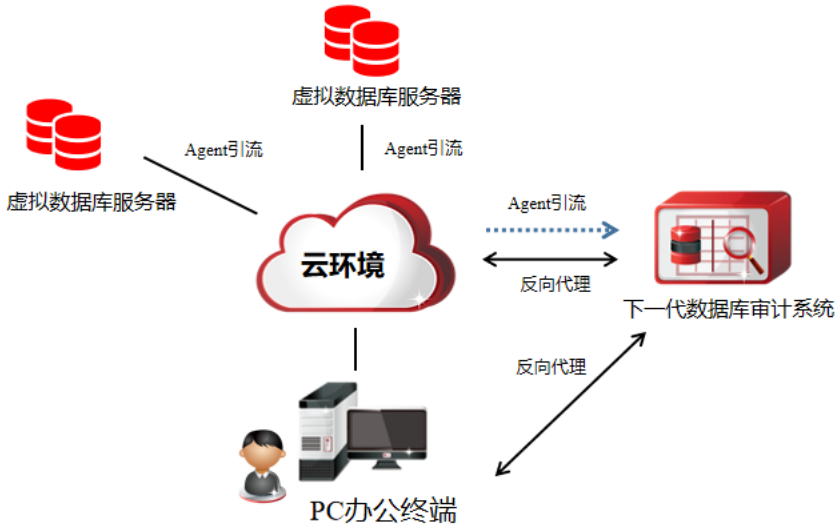
TA-DB 提供丰富灵活的报表统计模板，诸如等保、萨班斯法案等合规性报表模板。内置数十种业务统计场景，如 SQL 操作类型、SQL 响应时间、影响行数等，全方位满足等保、分保检查中的审计项要求。

系统内置报表任务，可周期性的生成日报、周报和月报；系统支持 PDF、WORD 等格式的报表文件导出，并可通过邮件发送至相关人员。此外，还支持根据业务要求，定制符合业务需求的业务报表。



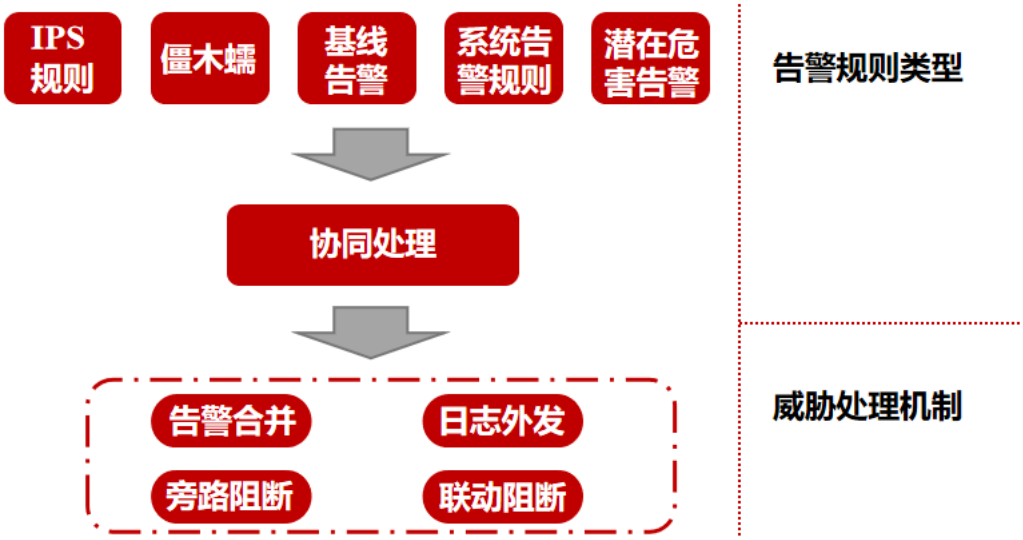
3.9 云环境审计支持

为了应对日益复杂的云环境，TA-DB 除了支持在云数据库上安装 Agent 引流进行审计外，还支持反向代理功能。通过内置的反向代理策略，获取客户端对云端数据库进行操作的流量，从而解析对数据库的操作。



3.10全场景协同联动

对产生的审计事件和告警事件，TA-DB 提供了全场景的安全响应机制。系统提供 8 个级别的告警设置，支持以 SYSLOG、SNMP 声光等方式外发响应事件，通过管控平台，使用 kafka、syslog、mail 等方式发送审计日志和规则告警信息到第三方平台，并可与第三方管理平台（如 SOC、态势平台）进行联动，支持旁路阻断、防火墙联动等方式阻断违规事件。



3.11可靠的系统管理

针对系统管理，TA-DB 提供了版本回滚、抓包工具、一键巡检等功能。并且在登陆过程中，可采用多种国密算法进行验证，最大程度上保证设备的安全可靠运行。

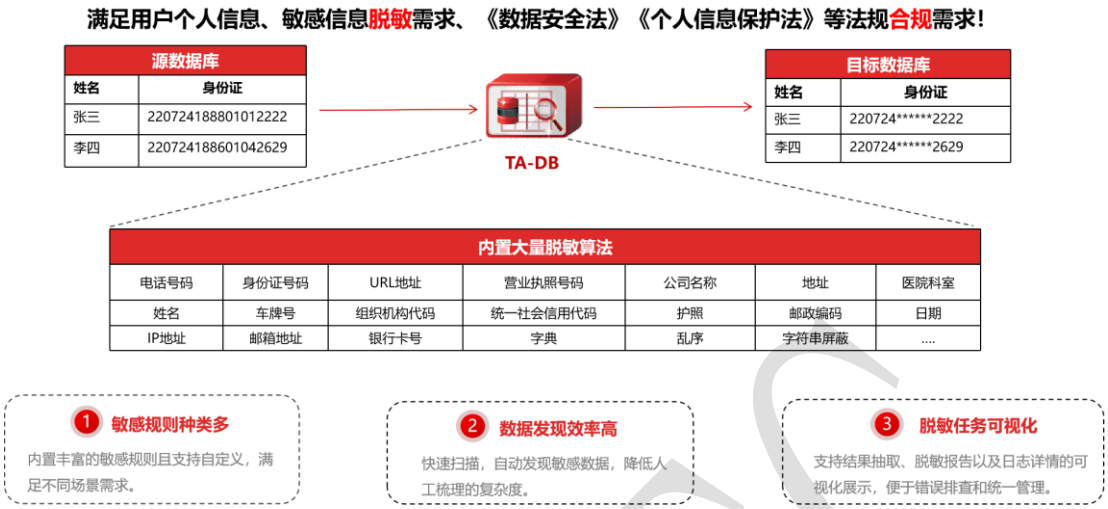
3.12灵活的双协议栈

系统全面支持 IPv6 协议族，能够在 IPv6 网络环境中实现 TA-DB 的所有功能，并且 TA-DB 通过了业界权威的 IPv6 Ready LogoII认证，并获得相关认证证书。

3.13高效的数据脱敏

系统内置高效的脱敏算法，通过脱敏模块对数据进行遮盖、变形、漂白，将敏感数据去标识化处理，隐藏真正的数据，为企业在系统开发、系统测试、产品培训和大数据应用等情

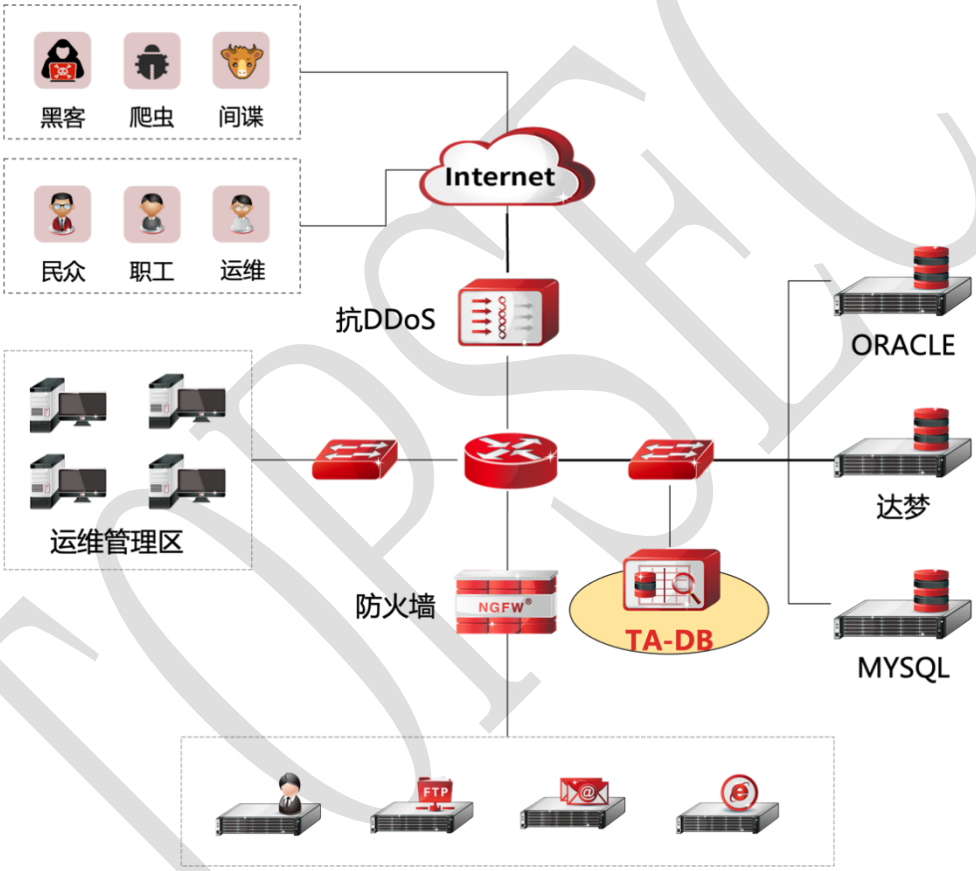
况下的数据的安全使用提供了保障。



4 部署模式

4.1 旁路部署

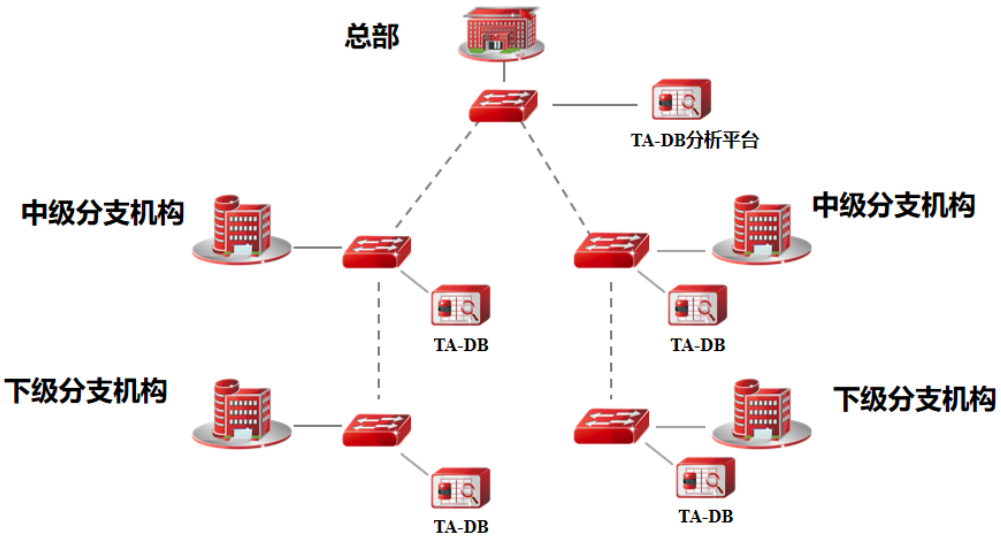
旁路部署是最常见的部署方式，将审计系统接到交换机的镜像口后，即可使用审计系统，系统上线方便快捷，不影响原有的网络结构。部署示意图如下：



4.2 级联部署

级联部署中每台审计系统都是一台独立运行的设备，审计自身的网络数据。上级设备可下发策略；上级设备也可查看下级设备的统计分析结果等。

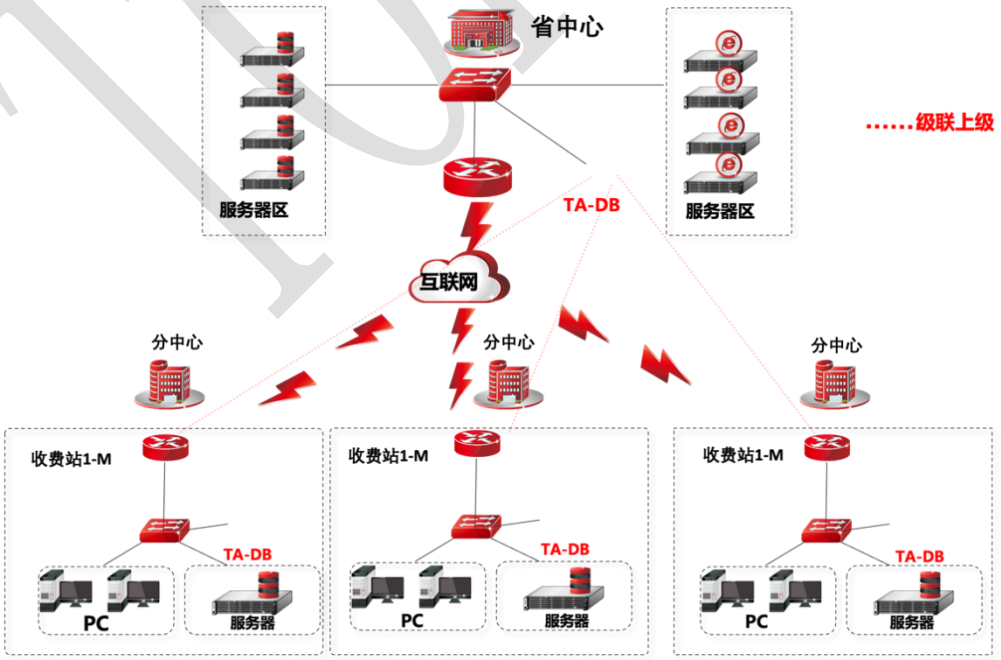
该部署模式能够适应客户网络结构，解决客户分级控制和审计的需求。部署示意图如下：



4.3 分布式部署

分布式部署中，利用了多台 TA-DB 设备分担用户整个网络数据库审计负荷，并采用高性能的集中管理中心，有效解决监控点分散，性能压力大的问题。

管理中心负责策略的下发，数据查询等。用户可根据自身情况，决定代理点是将审计事件发送给管理中心还是存储在代理点本地，无论事件是存储在管理中心还是代理点，管理员都可以通过管理中心的 WEB 界面，查询各个代理点的审计事件和统计分析结果等。部署示意图如下：



5 产品规格

TA-DB 为软硬一体件产品，同时提供命令行与 B/S 架构的系统管理平台供用户对系统进行全方位配置与管理。

说明	平台，级联部署	探针，单台部署
型号	天融信数据库审计系统 V3	
CPU	飞腾 D2000(2.3GHZ,8 核)	
操作系统	银河麒麟 V10(内核版本 4.19.90)	
内存	32GB	
硬盘	24TB、18TB、8TB、4TB，支持存储空间扩展	
网络接口	2 个千兆管理口（10/100/1000M 以太网电口）、4 个业务口（10/100/1000M 以太网电口）、4 个千兆光业务口（满配多模光模块）、2 个 10Gb 万兆光业务口（满配多模光模块）。	
USB 接口	2 个	
产品形态	2U 标准机架式设备	
冗余电源	标配模块化双电源	
净重	11.3Kg	
毛重	15.4Kg	
电压	AC100~240V	
频率	50~60HZ	
电流	5A-3A	
功率	550W	
运行温度	0℃~40℃	
存储温度	-40℃~55℃	
相对湿度	10%~90%RH 非凝结	

6 产品资质

证书名称	认证机构
计算机信息系统安全专用产品销售许可证 （增强级）	公安部网络安全保卫局
涉密信息系统产品检测证书	国家保密科技测评中心
计算机软件著作权登记证书	中华人民共和国国家版权局
中标麒麟软件 NeoCertify 认证 （兆芯版）	麒麟软件有限公司
银河麒麟软件 NeoCertify 认证 （飞腾版）	麒麟软件有限公司
飞腾 CPU 兼容性证明	天津飞腾信息技术有限公司
海光 CPU 兼容性证明	海光信息技术股份有限公司

声明

1．本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2．本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此种情况产生的差异为正常现象，产品功能或性能请以产品用户手册等资料为准。

3．本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息造成或可能造成他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。

RELIABLE NETWORK
SAFE WORLD
TOPSEC