

★完全公开



数据库审计与防护系统产 品白皮书

地址：北京市西城区西直门外南路26号院1号

邮编：100044

© 奇安信集团

股票简称：奇安信 股票代码：688561

● 版权声明

奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“本声明”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“本产品”）。如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分內容。您有责任定期检查免责声明部分的内容，以了解是否发生了变更。如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。

1. 您明确理解并同意，本产品按“现状”提供，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。
2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。
3. 您明确理解并同意，您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5)政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力或不可预见的情形造成的各类直接或间接损失，均不承担任何责任。
4. 对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。
5. 对于从非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。

6. 上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。
 7. 奇安信集团保留在不发布通知的情况下随时采取以下行动的权利：在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。
 8. 本声明受中华人民共和国法律的约束并依据其解释。
 9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。
-

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0.0	C	新建			

状态：C-创建，A-增加，M-修改，D-删除

数据安全分级标注说明

■ 数据分级	公开数据 ()	内部数据 (Y)	普通商秘 ()	核心商秘 ()
<p>*数据分级标注及说明：</p> <ol style="list-style-type: none">1、文档编写前，应标注数据安全级别，默认为内部；2、请根据文档内容评估数据安全级别，在对应数据级别 () 中填写 (Y) ；3、分级 TIPS: <p>【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；</p> <p>【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；</p> <p>【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；</p> <p>【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。</p> <p>更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips</p>				

目录

1 产品概述	1
1.1 产品简介	1
1.2 产品定位	1
1.3 产品形态及构架	1
2 产品功能	2
2.1 审计语句分析和翻译	2
2.2 关联审计，事件准确定位	2
2.3 双向审计	3
2.4 事件关联性分析	3
2.5 风险处理电子化	3
2.6 访问工具监控	4
2.7 事件场景还原	4
2.8 黑白名单审计	4
2.9 数据库备份审计	4
2.10 复杂语句审计	5
2.11 本地审计	5
2.12 关键字段值提取.....	5
2.13 查询细粒度.....	6
2.14 独特报表功能	6
2.15 高可用性	6
2.16 数据库资产自动扫描发现	6
2.17 攻击型风险识别，阻断其操作	7
3 特点与优势	7
3.1 广泛支持各行业主流数据库.....	7
3.2 字符型协议审计	8
3.3 关联审计精准定位到具体的操作人员	8
3.4 独立的审计模式	8
3.5 审计细腻度更深	8
3.6 分权管理	9
3.7 丰富的策略库	9
3.8 云架构下的审计	9
4 产品价值	9
4.1 协助通过各种合规检测.....	9
4.2 溯源分析，精准定责	10
4.3 资产数据安全防护	10

4.4 访问权限控制	10
5 应用场景.....	11
5.1 数据库操作行为监控和审计.....	11
5.2 防止敏感数据二次泄露.....	11
5.3 审计语句分析和翻译	11
5.4 风险旁路阻断	12
5.5 数据库风险预警	12
5.6 合规性报表.....	12
6 安装部署.....	13

1 产品概述

1.1 产品简介

奇安信网神数据库审计系统是一款软硬一体化产品，采用数据库深度报文协议解析技术 DPI 及流媒体分析技术 DFI 等，将数据库的各种访问操作，解析还原为数据库级的操作语句，通过预置的安全规则匹配，即可智能分析和监控访问者的各类正常、异常、违规操作，进行实时威胁预警，并对事件进行统计分析记录，多重身份定位，有效电子取证。

1.2 产品定位

奇安信网神数据库审计与防护系统对审计和事务日志进行审查，从而跟踪各种对数据库操作的行为，主要记录对数据库的操作、对数据库的改变、执行该项操作的人以及其他的属性。这些数据被记录到数据库审计与防护系统独立的平台中，并且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种操作历史，对我们分析数据库的各类正常、异常、违规操作提供证据。

1.3 产品形态及构架

奇安信网神数据库审计与防护系统其内部由报文采集模块、协议解析模块、规则匹配模块、入库模块、告警模块、数据存储模块、WEB 服务等几大模块组成。

数据库审计与防护系统采用层次化设计，分别为业务处理层、数据存储层、应用支撑层、业务逻辑层、用户表示层。业务处理层通过报文采集模块接受报文，经过报文重组后进行协议解析，对解析出来的 SQL、客户端 IP、数据库用户、应用账号等等进行规则库匹配，由告警模块对存在风险的操作进行告警，告警的方式由接口管理模块决定；如果规则库中配置了阻断动作，那么对匹配上该阻断的风险时由阻断处理模块进行阻断。数据存储层对风险和非风险的审计记录进行存储，由业务逻辑层进行统计分析汇总，并由用户表示层进行展示。

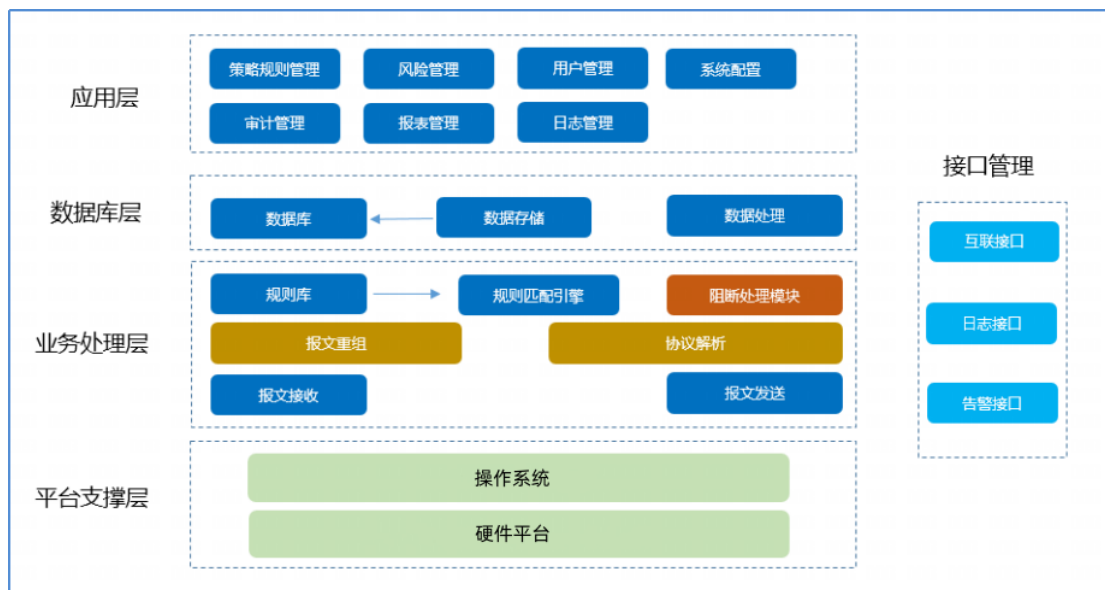


图 1-1 数据库审计与防护系统架构图

2 产品功能

2.1 审计语句分析和翻译

在实际项目中，有些单位有专门负责审计的机构，如在医院中，奇安信网神数据库审计与防护系统审计和操作权限由医院纪委监察室和信息科分别掌握，因数据库 SQL 语言及其它数据库语言如 M 语言的抽象性，非专业技术人员很难看懂语句的真实信息以及蕴含的风险，而专业技术人员不存在该问题，为更好的方便客户使用，奇安信网神数据库审计与防护系统提供了专业的数据分析和翻译界面。通过在配置中设置表和字段的中文别名，在翻译中以直观和易懂的语言显示审计的结果及语意关系，方便非专业技术人员的查看。

2.2 关联审计，事件准确定位

在信息安全及虚拟化背景时代下，单靠某一个信息去定位违规操作者已经成为不可能，如内网用户大多采用 DHCP 分配 IP 地址，没有做 IP-MAC 绑定及相应的准入规则，用户可通过更改操作系统名、IP 地址、MAC 地址等方式逃避追踪，传统的数据库审计定位往往局限于 IP 地址和 MAC 地址，很多时候不具备可信性。因此只有通过关联尽可能多的身份定位信息进行定位以及做一定的准入权限设

置，其审计结果才具有可靠性，才能作为电子证据。奇安信网神数据库审计与防护系统可以对 IP、MAC、操作系统用户名、使用的工具、应用系统账号等一系列进行关联分析，从而追踪到具体人。

2.3 双向审计

返回结果就是指某个查询操作所返回的数据，审计过程中可根据返回数据的内容、返回行数去直观的判断操作的危险性。奇安信网神数据库审计与防护系统可审计到双向数据，从客户端请求到服务器端的响应，做到双向审计。

2.4 事件关联性分析

奇安信网神数据库审计与防护系统可对响应事件进行关联，如根据 IP 关联出某段时间内该 IP 所触发的告警数量等；根据一段时间内的数据库或应用系统登录失败次数判断出暴力破解密码的可能性；根据账号的多次登录判断账号信息泄密或共享账号的可能性；相似 SQL 语句执行时间过长从而判断该语句设计的合理性等。根据事件关联性分析，自动涌现一批对客户具有实用价值的信息，帮助客户管理和维护好现有应用。

2.5 风险处理电子化

奇安信网神数据库审计与防护系统同其它应用系统一样，支持流程的标准化，当发生数据库安全事件后，数据库审计与防护系统将事件关键信息通过电邮、短信等风险发送给安全审计相关人员，在调查取证确认合法性后通过数据库审计与防护系统给出处置意见信息，以确定事件的结束。审计管理员日后可通过追溯安全事件处置信息确定有无包庇及不作为行为。

支持通过管控平台，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；

支持根据审计数据进行多维度统计，并生成、下载报表；

支持多台探针集中管控，支持在集中管控平台上对探针进行配置、升级、状态监控和日志查看，支持进行探针数据集中查询、策略规则匹配和数据分析。

2.6 访问工具监控

奇安信网神数据库审计与防护系统自动扫描连接数据库的访问工具。从访问数据库的源头进行分析，应用系统和客户端工具根据不同的数据库类型可通过 ODBC、JDBC、直连等方式连接数据库，直接连接工具如 Winsql, Plsql 及 CS 架构的客户端工具等。如发现审计记录中出现未知的数据库连接工具或出现规定之外的连接工具，审计员可根据工具监控记录分析出使用过该工具的 IP 及关联的操作记录，进而取证使用该工具的源头及操作的合法性。

2.7 事件场景还原

奇安信网神数据库审计与防护系统可根据审计日志，通过时间、端口等因素构建出事件的关联性及其现场，通过模拟回放，模拟出整个事件的行动轨迹，通过大屏幕显示可方便分析人员及技术人员通过回放线索，直观的追溯事件的前后关联性及其风险蕴含较深的操作行为。

2.8 黑白名单审计

奇安信网神数据库审计与防护系统可根据客户意见及实际审计情况，将 IP、操作语句、账号等相关信息加入黑白名单。同时，在应用系统中，因应用系统对应后台的 SQL 语句固定，一旦发现其中含有危险信息则可将对应的 SQL 加入黑名单，而一旦应用系统中有某些语句疑似风险操作但其实际并不产生危害则可加入白名单。

2.9 数据库备份审计

数据库备份是一个很危险的操作，同时也是保护数据安全的一个例行操作，奇安信网神数据库审计与防护系统可以针对不同方式、不同数据库之间的数据库备份操作行为进行审计，针对违规的备份操作行为及时告警于管理人员。

2.10 复杂语句审计

在不同数据库及应用系统中，很多值得传递都是通过变量进行，如在 oracle 数据库中有绑定变量，在其它数据库中也有变量一说。如审计不到变量则无法对 SQL 指令的危险性进行判断。奇安信网神数据库审计与防护系统可对不同数据库的不同变量进行审计。如：监控嵌套与长语句使用大量的条件判断与筛选，对数据精准查询和统计，防范敏感数据泄露。

2.11 本地审计

一、基于网卡流量的本地回环审计

指操作数据库的流量通过网卡的本地审计（如应用、navicat 运维工具和数据库在同一台服务器）

解决方案：数据库服务器上部署 agent，配置对应网卡的 IP、端口抓取网卡流量即可进行审计

二、基于 socket 管道通信的本地审计

进程间通信（IPC）不会经过任何网卡即可完成通讯，所以不需要指定 IP，仅用数据库用户名和密码就能访问数据库（如 sqlplus）。

解决方案：在本地管道通讯过程中，首先读取到管道文件，对客户端（如 sqlplus）底层操作指令完整获取，获取之后将关键信息进行存储或者转发给数据库审计设备，并对非法攻击者或者运维人员私自修改或者删除数据库相关关键文件进行记录审计，并在告警时，将具体的变化内容通知给相关人员，完成 socket 管道通信的本地审计。

2.12 关键字段值提取

奇安信网神数据库审计与防护系统可根据配置，自动提取 SQL 指令中某关键字段的值，如查询语句中涉及的时间范围、查询的条件。尤其是在金融、高值耗材等信息中，可通过查询条件查询出财产、费用、联系人等敏感信息，通过提取

关注字段的值，并通过该值设置规则，则可更精确的对数据库访问操作进行精确审计。

2.13 查询细粒度

奇安信网神数据库审计与防护系统支持对原始会话包的审计、展示、下载查看，支持以会话为单位的数据库操作过程详细记录，包括但不限于精确的时间点、来源网络地址、来源端口、客户端主机名、数据库实例名、数据库类型、目标地址、目标端口、客户端程序、数据库账号以及完整的操作行为详情。

2.14 独特报表功能

➤ 合规性报表

奇安信网神数据库审计与防护系统报表和根据合规性要求，输出不同类型的报表。例如，SOX 塞班斯合规报告。

➤ 策略定制化报表

根据审计人员关注的主要问题，定制符合需求的策略规则输出报告，使审计人员能够迅速的得到自己需要去审计信息。

提供全方位的策略规则匹配；数据库审计系统应满足等保三级要求。

2.15 高可用性

奇安信网神数据库审计与防护系统全方位确保设备本身的高可用性，主要包括：硬件级安全冗余、系统级防攻击策略、告警措施等。

2.16 数据库资产自动扫描发现

根据设定 IP 与端口范围以及网络报文协议解析，可以自动扫描出对应的数据库资产信息，一键添加保护对象，操作简单快捷，协助用户进行数据库资产梳理。

2.17 攻击型风险识别，阻断其操作

奇安信网神数据库审计与防护系统内嵌专业安全检测引擎，通过解析出的操作行为，与风险规则进行比对，及时发现、预警并阻断危害数据库的行为。数据库审计与防护系统内置数百种安全规则库，自动根据预设置策略，实现对风险会话操作的及时阻断做到事中控制。

3 特点与优势

3.1 广泛支持各行业主流数据库

奇安信网神数据库审计与防护系统作为全业务审计系统，支持各种数据库操作、网络操作行为的审计。如下图所示，包括：基于客户端的链接审计、基于 ODBC/JDBC 等链接访问、本地操作、网络操作等。

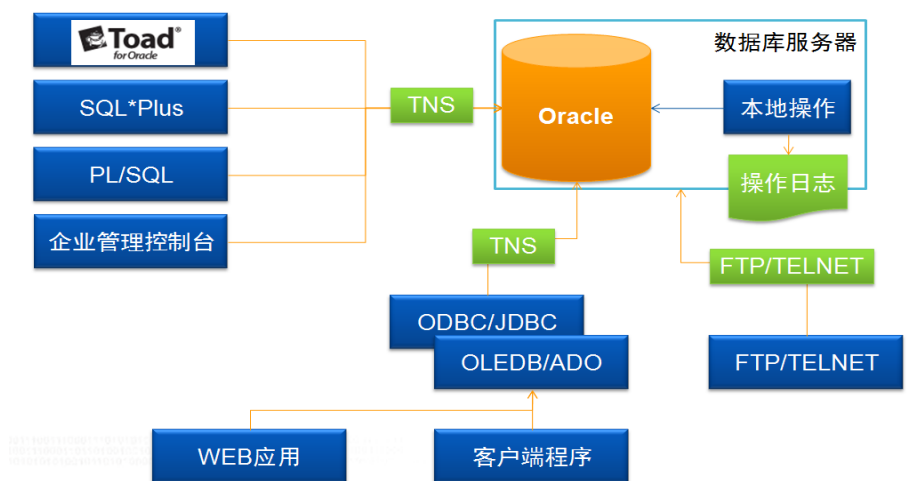


图 3-1 支持的审计类型

➤ 支持多种数据库类型：

- ✧ 支持主流数据库和国产化数据库的访问，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。
- ✧ Caché 五种工具操作行为全面支持的厂商，Caché 正在成为医疗行业高性能数据库应用场景的新宠；

- ◇ 同时支持多个系统数据库的审计；
- ◇ 同时支持不同类型的数据库的审计；
- ◇ SQL 处理性能35000SQL/S,支持20000字节的 SQL 语句进行完整审计和解析,保证审计日志的完整性和可靠性,无审计盲点;支持10个数据库集群资产;吞吐量4Gbps。

3.2 字符型协议审计

除支持对各种数据库访问审计外,数据库审计与防护系统还支持 SSH、FTP 等各种字符型协议对数据库服务器的访问,并可对其设置告警条件,如发现移动或下载数据备份文件时触发告警。

支持无需提供数据库的账号和密码,即可审计出 SQL Server 的 TDS 协议交互的全部数据。

3.3 关联审计精准定位到具体的操作人员

审计系统支持 B/S、C/S,以及带 COM/DCOM/COM+组件方式的三层关联审计。支持独创组件关联技术,将 url 信息与操作语句信息关联提取工号(账号),精准定位到具体的客户端操作人员。

3.4 独立的审计模式

在数据安全时代,独立的审计模式符合相关标准和法规的要求。奇安信网神数据库审计与防护系统采用独立的安全结构,通过交换机镜像完成数据的采集,不需要在应用系统、终端安装任何插件,其部署与运维不影响原有业务网络及应用。

3.5 审计细腻度更深

全面性:针对业务层、应用层、数据库等各个层面的操作进行跟踪定位,包括数据库 SQL 执行情况、数据库返回值等。

细粒度:精确到表、对象、记录内容的细粒度审计策略,实现对敏感信息的

精细监控。

独立性：基于独立监控审计的工作模式，实现了数据库管理与审计的分离，保证了审计结果的真实性、完整性、公正性。

3.6 分权管理

安全法规要求审计设备具有一定的权限控制，奇安信网神数据库审计与防护系统系统设置了权限角色分离，如系统管理员负责设备的运行设置；审计员负责查看相关审计记录及规则违反情况；规则配置员负责数据库审计安全规则的配置等。

3.7 丰富的策略库

奇安信网神数据库审计与防护系统根据不同的行业应用提供了不同的策略库，如：根据 drop、delete、alter 等危险操作行为制订了数据库危险操作策略，有如根据不同工具的数据库备份信息制定了数据库备份策略库等。

3.8 云架构下的审计

出于节能、环保及云计算技术等因素的考虑，现在越来越多的客户将应用系统及数据库服务部署在虚拟架构的同一物理平台中，数据报文之间的流动在虚拟环境内部进行，不通过物理交换机，而现有的审计技术大多采用旁路镜像的方式，在物理架构及部署上因“看不到”数据报文无法实现对虚拟平台的数据库服务器进行审计，本公司率先通过报文引流技术解决“看不到”报文的问题，攻克了对云平台架构的数据库审计技术。

4 产品价值

4.1 协助通过各种合规检测

帮助用户满足等保、分保等合规要求，各政府及行业对于信息安全越来越重视，也提出了很多的相关标准来确保各单位的网络安全。政府的行政事业单位或

者国有企业则有遵循等保护、分保的合规性要求。奇安信提供了一套独立的审计方案，有助于完善组织的内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过审计。

等级保护是公安部、国家保密局等多个权威部门联合制定的国家信息安全标准，也是目前我们推广最为广泛、对国家信息安全影响最大的安全标准。推动等级保护这对于促进信息化健康发展，保障各行各业体制改革，维护公共利益、社会秩序和国家安全具有重要意义。

综上所述，国家信息安全等级保护主要从以下三方面来要求：

- ◇ 发现： 制定策略，审计覆盖每个用户，可实时报警
- ◇ 审计： 有专门的审计工具
- ◇ 取证： 保护措施，安全事件

4.2 溯源分析，精准定责

奇安信网神数据库审计与防护系统主要通过业务关联功能和审计功能，从各个维度进行统计分析、结合原始用户操作审计记录，提供原始数据的快速检索能力，让用户能快速确认问题的来源，并将安全事件进行精准定位、追责到人，溯源取证。

4.3 资产数据安全防护

奇安信网神数据库审计与防护系统能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。通过对用户访问数据库行为的记录、分析和汇报，帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

4.4 访问权限控制

奇安信网神数据库审计与防护系统可针对哪些持有特权账号进行了误操作或者不法行为时，特别是运维人员，可对该用户的部分操作进行阻断控制并及时

告警，从而降低影响以及损失。同样也可以通过控制只有特定的访问 IP 范围才能对数据库进行访问，从而阻断那些非法分子进行访问，提高数据资产安全。同时，数据库审计与防护系统亦可梳理当前所有账号的权限控制，规范其资产的权限使用以加强数据库账号权限管理。

5 应用场景

5.1 数据库操作行为监控和审计

针对数据库操作途径众多，有应用系统、运维工具，还有直连数据库进行操作；人员众多等，而且在操作过程中，无法可视化知道具体的操作行为和具体的操作内容，操作行为是否有危险，是否符合权限，不能及时行为分析；

通过奇安信网神数据库审计与防护系统的可视化行为监控审计与关联分析能力，对从客户端请求信息到服务器端响应回复信息双向审计，实现“终端”、“应用服务器”、“数据库”三层关联，精准审计定位到人，完成帮助客户管理和维护好现有应用，如根据 IP 关联出某段时间内该 IP 所触发的告警数量等。

5.2 防止敏感数据二次泄露

数据库操作行为精准审计的过程中，会将 SQL 语句的请求的具体请求结果返回，这些具体的内容信息中包含了定性为敏感的数据信息，若将返回结果直接展示给不同的审计人员，会造成数据库中的敏感数据二次泄露。

通过奇安信网神数据库审计与防护系统的敏感数据识别与防护能力，在进行数据库安全审计前，数据库审计与防护系统自动扫描出敏感数据分布信息，用户根据扫描出的敏感数据信息设置访问规则，客户端访问数据库时触发了敏感数据访问规则，在记录返回结果数据时，对涉及到的敏感数据进行掩码处理，从而防止敏感数据的二次泄密。

5.3 审计语句分析和翻译

有些单位设有专门负责审计的部门或机构，如在医院中，所有的数据库审计

结果由信息科保存，纪委监察室进行监管审计，因存储的数据库审计结果数据，是数据库 SQL 语言信息，具有抽象性和专业性的特点，纪委人员处于非专业的数据库管理人员，很难看懂语句的真实信息以及蕴含的风险。

通过奇安信数据审计翻译功能，在配置中设置表和字段的中文别名，在翻译页面，将 SQL 语句翻译成直观和易懂的语言来显示审计的结果及语意关系，方便非专业技术人员的查看。

5.4 风险旁路阻断

数据库受到内外部人员违规操作时，虽然已部署了网络防火墙，堡垒机等其他网络安全措施，但这些只是用于网络安全操作行为防范，这些设备直接串联在业务系统的网络中，在执行安全防范策略时，直接影响到业务系统的正常运行。

数据审计具备通过旁路侦听和 Agent 引流的方式对访问数据库的数据流进行采集、分析和识别，并对识别的行为和内容进行存储、分析、统计和查询；

使用数据库审计的旁路阻断功能，解决因执行网络安全操作策略时造成的业务系统不可用的问题，审计系统不串联在业务系统中，通过 SQL 报文的解析，在发现数据库的违规操作时，直接阻断当前的会话操作，不执行网络的阻断。

5.5 数据库风险预警

当数据库出现风险时，需要第一时间通知管理员处理风险，同时发消息知会领导；

数据库审计与防护系统可设置告警策略，针对不同的风险等级设置不同的告警接收人，可通过邮件、短信等方式进行告警；如果本来就有网管系统，也可以通过 snmp 的方式告警。

5.6 合规性报表

单位现在需要进行等保合规的建设，在进行等保合规的日常检查过程中，等保合规报表的生成时没有固定的模板，每次手动进行报表的统计，在统计过程中很容易出现统计项的遗漏。

通过系统自带了等保合规报表的统计模板，在任何时间、任何状态下都能够快速，自动的导出符合等保要求的数据库操作行为审计报表。

6 安装部署

为了完全不影响数据库系统自身运行与性能，奇安信网神数据库审计与防护系统应支持采用旁路监听模式，具体可分为核心交换机网络监听模式、网桥模式和数据库系统主机上实施监听模式，另外在设备部署时，可根据客户实际环境使用需求，以集中管控平台为基础，通过审计探针实现数据抓取，而集中管控平台根据本身原有的 4T 存储容量，可以根据审计探针实际情况扩展硬盘存储，最高可扩展至 48T，以保证满足数据存储合规要求。

旁路部署模式：

通过在核心交换机上设置端口镜像模式或采用 TAP 分流监听模式，使安全审计引擎能够监听到所有用户通过交换机与数据库进行通讯的全部操作。具体部署结构示意图如下图所示：

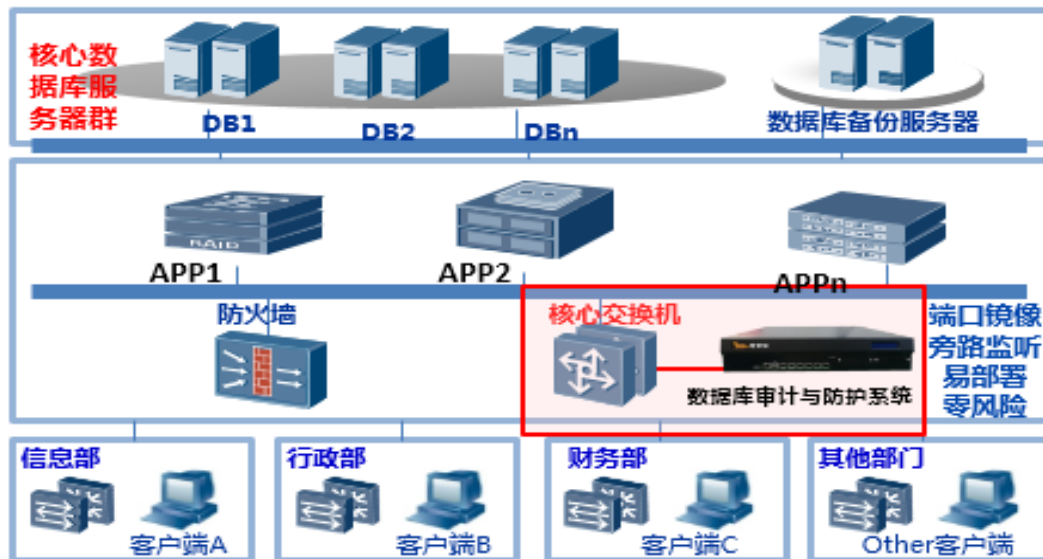


图 6-1 数据库审计与防护旁路部署模式示意图