**360 数据库审计系统**

**产品白皮书**

**360 企业安全集团**

**2018 年 7 月**

**目录**

[1 前言 4](#_bookmark0)

[2 为什么需要数据库审计 4](#_bookmark1)

[2.1 数据库面临的威胁 4](#_bookmark2)

[2.2信息安全等级保护要求 6](#_bookmark3)

[2.3 传统防护手段捉襟见肘 8](#_bookmark4)

[3 数据库审计产品概述 9](#_bookmark5)

[3.1 系统架构 9](#_bookmark6)

[3.2 部署方案 11](#_bookmark7)

[4 产品技术特点 12](#_bookmark8)

[4.1 独立的审计模式 12](#_bookmark9)

[4.2 审计细腻度更深 13](#_bookmark10)

[4.3 审计语句分析和翻译 13](#_bookmark11)

[4.4 防二次泄密 14](#_bookmark12)

[4.5 分权管理 14](#_bookmark13)

[4.6 事件准确定位 15](#_bookmark14)

[4.7 返回结果 15](#_bookmark15)

[4.8 事件关联性分析 15](#_bookmark16)

[4.9 字符型协议审计 16](#_bookmark17)

[4.10 风险处理电子化 16](#_bookmark18)

[4.11 访问工具监控 17](#_bookmark19)

[4.12 事件场景还原 17](#_bookmark20)

[4.13 黑白名单审计 18](#_bookmark21)

[4.14 丰富的策略库 19](#_bookmark22)

[4.15 数据库备份审计 19](#_bookmark23)

[4.16 变量审计 19](#_bookmark24)

[4.17 关注字段值提取 20](#_bookmark25)

[4.18 查询细腻度 20](#_bookmark26)

[4.19 独特报表功能 20](#_bookmark27)

[4.20 自身安全 21](#_bookmark28)

[4.21 非法操作协同阻断 21](#_bookmark29)

[4.22 集中管理平台的技术特点 22](#_bookmark30)

[5 SECFOX技术创新点 24](#_bookmark31)

[5.1 数据库状态监控 25](#_bookmark32)

[5.2 数据库态势感知 25](#_bookmark33)

[5.3 云架构下的审计 25](#_bookmark34)

[5.4 身份加密报文的破译 25](#_bookmark35)

[5.5 首创后关系型数据库的审计 27](#_bookmark36)

[5.4 大数据安全监控行业领先 28](#_bookmark37)

[5.5 首创工业控制实时数据库的安全监控 30](#_bookmark38)

[6 产品资质 32](#_bookmark39)

# 1 前言

随着信息化的深入和普及，各行各业对信息系统的依赖性越来越强，信息系统 中的数据也逐渐成为了企业的生命。数据的不准确、不真实、不一致、重复杂乱等 就会影响企业的健康。

网神SecFox安全审计系统（“以后简称SECFOX”）从合规性、降低风险的 角度，针对数据库的所有操作进行一些列的检查、分析，确保数据安全性。

# 2 为什么需要数据库审计

数据库安全事故的层出不穷，诸如银行内部数据泄漏造成资金失密、信用卡信 息被盗用导致的系用卡伪造、企业内部机密数据泄漏引起的竞争力下降、医疗患者 信息泄漏导致患者被“监控”……，这些情况无不说明了应用系统审计的重要性。

## 2.1 数据库面临的威胁

数据库做为企业的核心资产，承载企业重要信息，时时刻刻都面临着各类风 险，如下所示的风险一直威胁着数据库安全：

* **威胁 1 - 滥用过高权限**

当用户（或应用程序）被授予超出了其工作职能所需的数据库访问权限时，这 些权限可能会被恶意滥用。例如，一个大学管理员在工作中只需要能够更改学生的 联系信息，不过他可能会利用过高的数据库更新权限来更改分数。

* **威胁 2 - 滥用合法权**

用户还可能将合法的数据库权限用于未经授权的目的。假设一个恶意的医务人

员拥有可以通过自定义 Web 应用程序查看单个患者病历的权限。通常情况下， 该 Web应用程序的结构限制用户只能查看单个患者的病史，即无法同时查看多个 患者的病历并且不允许复制电子副本。但是，恶意的医务人员可以通过使用其他客 户端（如MS-Excel）连接到数据库，来规避这些限制。通过使用 MS-Excel 以及 合法的登录凭据，该医务人员就可以检索和保存所有患者的病历。

* **威胁 3 - 权限提升**

攻击者可以利用数据库平台软件的漏洞将普通用户的权限转换为管理员权限。 漏洞可以在存储过程、内置函数、协议实现甚至是 SQL语句中找到。例如，一个 金融机构的软件开发人员可以利用有漏洞的函数来获得数据库管理权限。使用管理 权限，恶意的开发人员可以禁用审计机制、开设伪造的帐户以及转帐等。

* **威胁 4 - SQL 注入**

在SQL注入攻击中，入侵者通常将未经授权的数据库语句插入（或“注入”） 到有漏洞的SQL数据信道中。通常情况下，攻击所针对的数据信道包括存储过程和 Web应用程序输入参数。然后，这些注入的语句被传递到数据库中并在数据库中 执行。使用SQL注入，攻击者可以不受限制地访问整个数据库。

* **威胁 5 – 日志记录不完善**

自动记录所有敏感的和/或异常的数据库事务应该是所有数据库部署基础的一 部分。如果数据库审计策略不足，则组织将在很多级别上面临严重风险。

薄弱的身份验证方案可以使攻击者窃取或以其他方法获得登录凭据，从而获取

合法的数据库用户的身份。攻击者可以采取很多策略来获取凭据。

* **威胁 7 - 备份数据暴露**

经常情况下，备份数据库存储介质对于攻击者是毫无防护措施的。因此，在若 干起著名的安全破坏活动中，都是数据库备份磁带和硬盘被盗。防止备份数据暴露 所有数据库备份都应加密。实际上，某些供应商已经建议在未来的 DBMS产品中 不应支持创建未加密的备份。建议经常对联机的生产数据库信息进行加密，但是由 于性能问题和密钥管理不善问题，这一加密方法通常是不现实的，并且一般被公认 为是上文介绍的细化的权限控制的不理想的替代方法。

## 2.2信息安全等级保护要求

《信息安全等级保护管理办法》 要求组织对信息系统分等级实行安全保护， 其中明确要求计算机信息系统创建和维护受保护客体的访问审计跟踪记录。

**数据库审计本身就是一个信息安全防范问题，政府机关、医院等重要的信息系 统属于三级，属于公安机关强制性信息安全防护要求等级。**

 **等级保护三级基本要求**

 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审 计；

 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和 结果等；

 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

 **等保三级测评要求**

应设置安全审计员，询问应用系统是否有安全审计功能，对事件进行审计的 选择要求和策略是什么，对审计日志的保护措施有哪些；

 应检查主要应用系统，查看其当前审计范围是否覆盖到每个用户；

应检查主要应用系统，查看其审计策略是否覆盖系统内重要的安全相关事 件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源 的异常使用、重要系统命令的使用等；

应检查主要应用系统，查看其审计记录信息是否包括事件发生的日期与时 间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求 的来源、事件的结果等内容；

应检查主要应用系统，查看其是否为授权用户浏览和分析审计数据提供专 门的审计分析功能，并能根据需要生成审计报表；

 应检查主要应用系统，查看其是否能够对特定事件指定实时报警方式；

应测试主要应用系统，可通过非法终止审计功能或修改其配置，验证审计进 程是否受到保护；

应测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件，查 看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况和记录情况与 要求是否一致；

应测试主要应用系统，试图非授权删除、修改或覆盖审计记录，验证安全审 计的保护情况与要求是否一致

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

## 2.3 传统防护手段捉襟见肘

目前众多行业还没有很好的措施来防范数据库攻击，而是通过传统的手段，通 过数据库自身审计产生的日志来分析，但是核心数据库自身的审计功能对数据库性 能影响较大，审计权限和操作权限也没有分离，对这种数据库自身审计产生的日 志，分析工作繁琐、人力投入大、审计信息易被篡改或泄漏等。大量的信息安全维 护工作分散到不同机构和部门的不同人员，部分开发、维护工作外包给合作的第三 方公司及人员，日常运维过程中普遍存在维护人员较多、缺乏严格的资源授权管理 审核、操作不透明、缺乏有效的技术手段来监管，代维人员操作、操作无审计等诸 多问题。

综上所述，我们了解到数据库安全防护存在以下风险：

◆ 数据库自身审计影响数据库服务器性能；

◆ 数据库自身审计日志分析工作繁琐、投入人力大、信息易被篡改或泄漏；

◆ 数据库维护人员权限没有控制起来；

◆ 对数据库的所有操作没有全面审计系统进行监管；

◆ 第三方工具直接访问数据库；

◆应用系统没有做相应的权限控制，敏感信息没有屏蔽，发生高危操作时没有

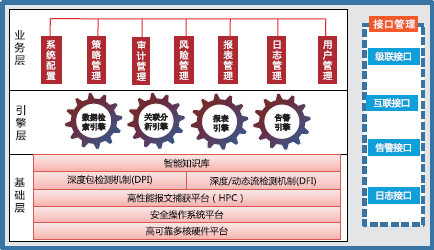
日志记录。

# 3 数据库审计产品概述

SECFOX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。一 般审计主要记录对数据库的操作、对数据库的改变、执行该项目操作的人以及其他 的属性。这些数据库被记录到SECFOX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 变化，对我们分析数据库的各类正常、异常、违规操作提供证据。

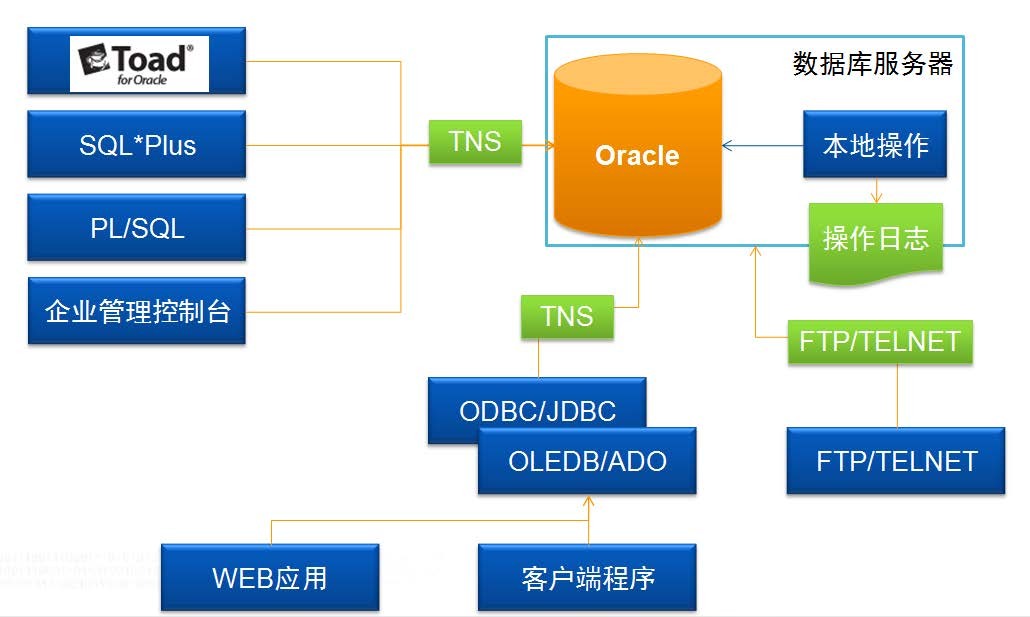
## 3.1 系统架构

网神SecFox安全审计系统由基础层、引擎层、业务层和接口管理层组成。其 中，基础层和引擎层共同构成了网神领先于同行产品的后台架构，该架构可概括为 “一库”“二机制”、“三平台”、“四引擎”。



网神SECFOX作为全业务审计系统，支持各种数据库操作方案、网络操作方

式。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。



* **支持多种数据库类型：**

* 同时支Oracle 8/9/10/11、DB2、INFORMIX、SYBASE、Microsoft SQL Server 97/2000/2005/2008、MYSQL、POSTGRESQL、 CACHE；

**国内为数不多支持的厂商，cache正在成为高性能数据库应用场景的新 宠等**

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



不同数据库版本及品牌采用的数据库应用协议各不相同，主要反应在报文协议格式及数据

编码上。针对不同数据库的审计支持，关键在于审计的深度、快速响应的技术实力以及不漏 审、不误审等。

## 3.2 部署方案

为了完全不影响数据库系统自身运行与性能，数据库安全审计系统应支持采用 旁路监听或模式，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。

* **交换机网络监听模式**

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 如图3.2.1所示。

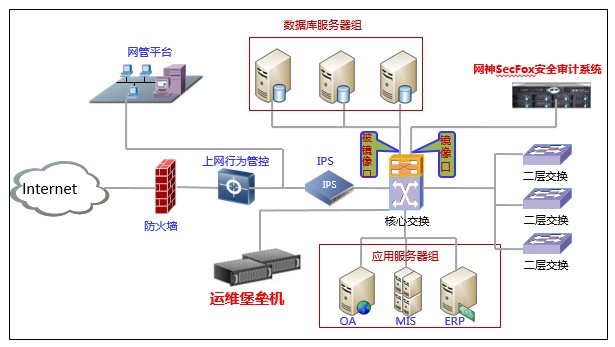
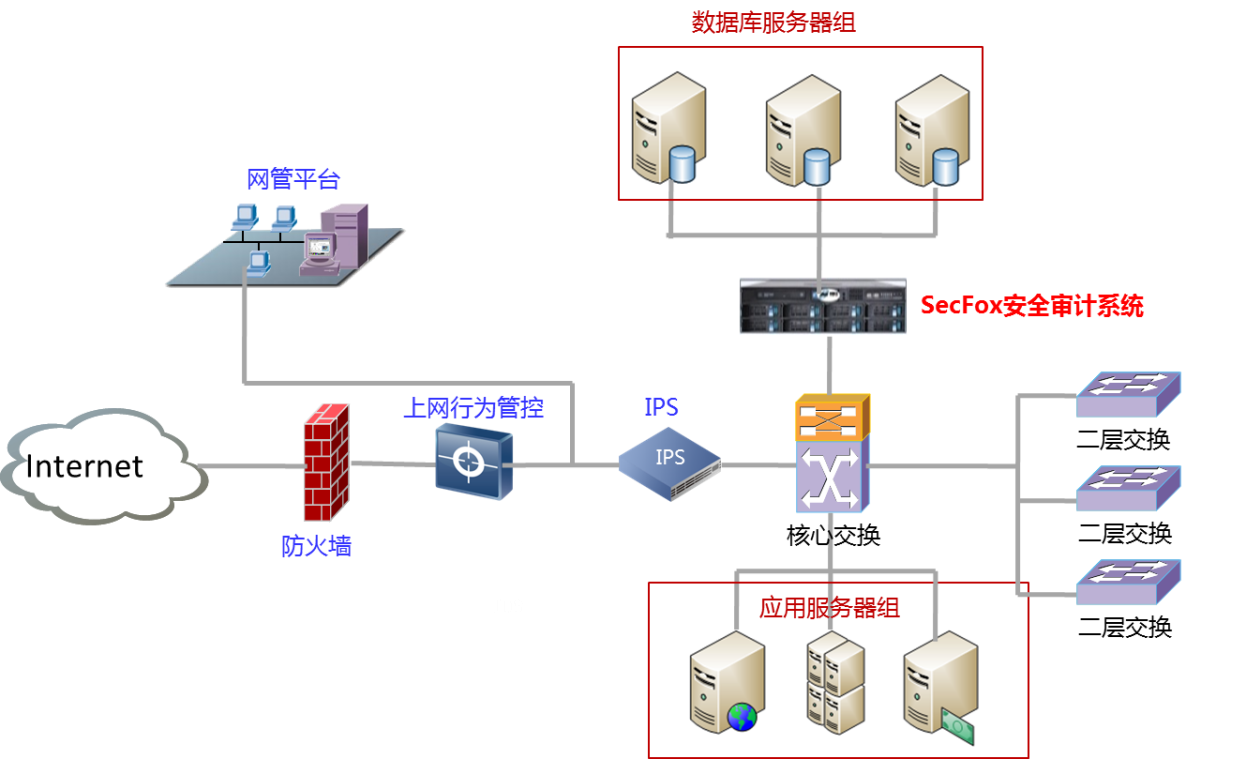


图3.2.1 交换机网络监听模式审计系统部署示意图

* **串联阻断模式**

通过将SecFox设备串联至数据库服务器前端，做了数据库网关，所有访问数

据库用户流量需先经过SecFox设备



* **集中管理平台部署模式**

过去在大型审计项目集中管理中，无法实现对数据库审计设备或防统方系统的 集中管理、维护，监控、预警 ，审计中心很难得到有效的汇总报告，设备出现故 障无法及时准确定位、权限分散的管理模式使管理维护成本居高不下等问题，网神 SecFox提供了业界最为领先的数据库审计或防统方集中管理和技术手段，彻底解 决了大型数据库审计项目或大型区域医疗防统方系统面临的部署、管理、监控、预 警以及日志方面的问题。

# 4 产品技术特点

## 4.1 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。网神SECFOX

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网络及应用。

同时，网神SECFOX采用三权分立的模式，这使得数据库维护或开发小组，安 全审计小组的工作进行适当的分离。而且，审计工作不影响数据库的性能、稳定性 或日常管理流程。审计结果独立存储于网神SECFOX自带的存储空间中，避免了数 据库特权用户或恶意入侵数据库服务器用户，干扰审计信息的公正性。

## 4.2 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。

## 4.3 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，数据库审计系 统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，网神SECFOX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。



审计语句的翻译和分析在清楚数据库表和字段结构的情况下进行，目前网神SecFox已经掌 握多家知名HIS厂家的数据库表结构信息，因各项目实际情况影响，需要对已有数据库表结构 信息进行纠正。语句的翻译和分析根据别名设置及数据库SQL或CACHE数据库M语言的语法语 意进行逻辑性分析及字段替换。

## 4.4 防二次泄密

在对数据库查询操作返回结果的审计中，返回信息包含了重要的敏感的信息， 一旦被审计人员看到会造成信息的二次泄密，同时也会增加审计人员泄密敏感信息 的可疑性。对审计结果中敏感字段进行系统级隐秘设置，可减少审计人员自身泄露 敏感信息的可能性，同时也增加了数据的安全性和保密性。



数据库审计系统作为一个记账工具，其本身不应该具有查看隐秘数据，泄露保密信息的功 能，从安全角度出发，网神SECFOX默认屏蔽了返回数据，只保留了返回值，以确定该操作执 行成功或失败。

## 4.5 分权管理

安全法规要求审计设备具有一定的权限控制，网神SECFOX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。

## 4.6 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。网神SECFOX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。

## 4.7 返回结果

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。网神SECFOX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。

## 4.8 事件关联性分析

网神SECFOX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。



事件关联性通过一定的策略配置，关联组合各有用信息从而体现出其价值。

## 4.9 字符型协议审计

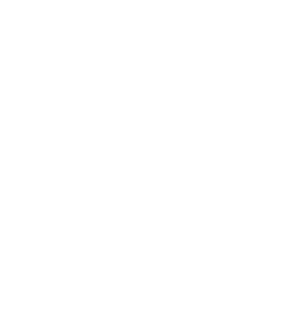
除支持对各种数据库访问审计外，网神SECFOX还支持TELNET、FTP等各种 字符型协议对数据库服务器的访问，并可对其设置告警条件，如发现移动或下载数 据备份文件时触发告警。



如果您还想要支持对其他协议访问数据库应用系统的审计时，如远程桌面等，建议您采购 网神的运维审计模块SECFOX-M。

## 4.10 风险处理电子化

网神SECFOX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，网神SECFOX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网神SECFOX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。



**无风险需 要有权人 确认并签**

**字**

**确认告警**

图4.10 风险告警处置流程

## 4.11 访问工具监控

网神SECFOX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。

## 4.12 事件场景还原

网神SECFOX可根据审计日志，通过事件、端口、端口等因素构建出事件的关 联性及现场，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风险蕴含较深

的操作行为。



事件场景还原模拟SQL指令的执行及结果的返回，通过时间线索、会话端口、执行语句先 后的关联关系，构建出事件前后的SQL之间逻辑关系，方便进行直观的分析。

## 4.13 黑白名单审计

网神SECFOX可根据客户意见及实际审计情况，将IP、操作语句、账号登相关 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。

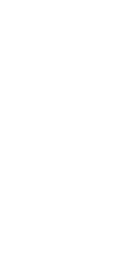


图4.13白名单审计示意图



通过黑白名单设置，可减少维护人员的工具量。

## 4.14 丰富的策略库

网神SECFOX根据不同的行业应用提供了不同的策略库，如在医疗行业，根据 不同HIS厂家的表和字段结构信息制定了符合不同HIS厂家的防统方策略库。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。



网神SECFOX提供了细腻度更高的规则设置界面，用户可根据规则设置定义出自己想想要 的策略已达到不同的目的。

## 4.15 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，网 神SECFOX可以针对不同方式、不同数据库之间的数据库备份进行审计，数据库备 份意义重大，如数据库备份文件被盗或数据库被备份到脱离控制的某地，大量数据 就可以离开内部网络单独建立数据库服务器进行脱机查询，如不针对备份操作进行 严格控制及设置告警，则可能数据丢失泄露被广而告之都无法觉察，严重影响企业 声誉，而数据库管理者也会因为失职而处罚。

## 4.16 变量审计

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。网神SECFOX可对不同数据库的不同变量进行审计。

## 4.17 关注字段值提取

网神SECFOX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。由其是在金融、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。

## 4.18 查询细腻度

网神SECFOX拥有丰富的查询条件，用户可基于IP地址、会话端口、关键字、 涉及的关键表、符合的规则名、操作系统的用户名、计算机名、使用的工具名、语 句的长度、语句的执行时间等设置查询和统计分析条件，细腻度越高，就越容易进 行精确查询，在大数据量的背景下查询出所需要的精准信息。

## 4.19 独特报表功能

* **合规性报表**

网神SECFOX报表和根据合规性要求，输出不同类型的报表。例如，可根据等

级保护三级要求，输出符合等保相关项目满足的度的报表。

* **策略定制化报表**

根据审计人员关系的主要稳定，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。

* **定时报表**

根据时间及报表内容定制自动报表发送策略，管理人员可定时定期收到网神

SECFOX自动发送的报表。

* **报表加密**

网神SECFOX可针对报表进行加密，防止非法权限用户查看审计报表。

## 4.20 自身安全

网神SECFOX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。

## 4.21 非法操作协同阻断

阻断即中断正在进行的数据库访问会话，在数据库审计的过程中，当发生一些 非法操作如：恶意备份、恶意查询敏感数据、查询时间过长导致数据库服务性能缓 慢时都需要及时的终端该操作行为，网神SECFOX可与交换机、堡垒机等安全设备 联动，实现对风险会话操作的实时阻断做到事中控制。

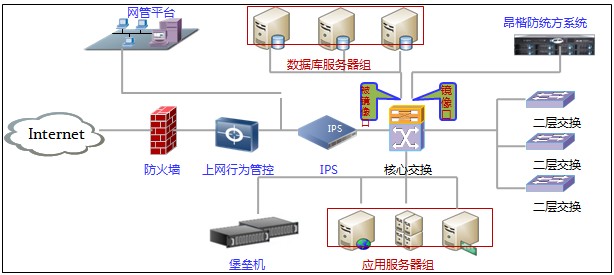


图4.21 协同阻断部署示意图



阻断本身是一个风险操作，如随意阻断或误阻断，容易影响应用系统的正常使用，网神 SECFOX本身不做阻断功能，对需要实现阻断功能的客户，网神SECFOX设备可提供接口与信 号给其它安全设备，协同合作实现联动和阻断。

## 4.22 集中管理平台的技术特点

网神集中管理平台的部署将解决私自隐瞒、处理统方风险日志，不上报； 缺 少指导，风险规则设置不规范，风险数太多，疲于处理风险； 风险不及时处理或 很少上线查看防统方系统审计情况； 设置白名单、规则等，规避数据库审计或防 统方系统对自身的审计； 数据库审计或防统方系统处于闲置状态，为应付上级检 查才上线等问题。

* **快速部署，集中管理**

审计中心可通过集中管理平台，实时的监控各分支节点的系统运行、在线情

况；

* **实时监控各点风险告警情况**

在集中管理平台下发告警策略给各分支节点，一旦有风险操作发生，集中管理

平台可同时收到告警信息，了解实情； 各审计点数据库审计系统管理员只能查看不允许修改上级下发的告警策略，避

免下级不报、瞒报风险告警情况；

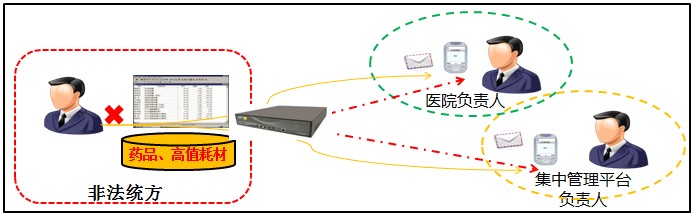


图4.22.1告警示意图

* **实时监控各审计点规则应用情况**

查看各审计点设置的数据库审计规则应用情况； 监控各审计点的数据库审计 规则设置是否合规，是否排除了对管理者本身的审计； 指导下级审计点的风险规 则设置。



**规则是否被正 规则是否设置**

**规则的设置是**

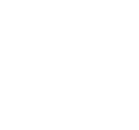


图4.22.2规则监控示意图

* **监控各审计点对风险的处理情况**

查看已处理和未处理的告警，根据风险发生时间、风险处理时间判断使用者对 风险处理的及时介入情况，尽早的介入对非法统方风险事故的处理可以将风险导致 的损失降到最低；

上级不监督，责任人不重视，数据库审计系统很容易成为摆设，监控医院风险 处理的及时性可预防不作为、走形式的不良风气；

* **监控各审计点的的白名单设置**

网神SECFOX设置了访问者白名单，可对访问者IP、数据库用户、操作语句等

作为白名单的条件，其目的是排除一些属于正常操作的疑似非法行为。通过集中管 理平台对各分支节点白名单的监控，可避免数据库审计系统管理者通过白名单功能 规避数据库审计系统的审计而进行风险操作。

* **各审计点状态管理**

监控各节点数据库审计系统的设备运行状态，如CPU、内存使用情况，运行时

间等，一旦设备不受控即可发出告警； 监控各节分支节点审计程序运行情况。如审计口有无数据，是否停止审计等； 添加、修改节点的数据库审计系统信息；

* **报表集中管理**

通过获取各节点数据库审计系统关键信息汇总生成各种报表；

* **预留接口**

可与上一级系统进行互联。

可作为二次开发之用；



集中管理平台的部署需要考虑网络连通性、网络带宽、实时性等问题。

# 5 SECFOX技术创新点

## 5.1 数据库状态监控

能够主动监控MySQL、Oracle、sqlserver、mongodb、redis数据库的状 态，可以对数据库服务器运行状态进行实时的监控与记录，主动发现数据库异常

## 5.2 数据库态势感知

基于环境动态，整体地洞悉安全风险，以数据为基础，从全局视角提升对安全 威胁的发现识别、理解分析。旨在帮助数据库管理人员、审计人员对系统运行状态 实时监控，及时发现各种异常和危险操作，为整体信息安全管理提供决策依据。

## 5.3 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边镜像的方式，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，网神SecFox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



在一些虚拟环境中，有将数据库服务器和应用服务器部署在同一物理机上的情况，如上图 虚拟环境A；也有将数据库服务器及应用服务器部署在不同物理机上，如上图虚拟环境B。

## 5.4 身份加密报文的破译

在数据库审计的过程中，我们经常会遇到不同的数据库应用协议及不同的数据

库版本，如在微软SQLServer2005及以上版本中，采用了加密协议加密了访问者 的身份信息，对数据库审计过程中的访问者身份识别带来了很大的难度，网神 SecFoxSECFOX系统发明了对数据库访问报文中身份加密内容的破译技术 ，实现 了对身份加密信息的破解和提取。

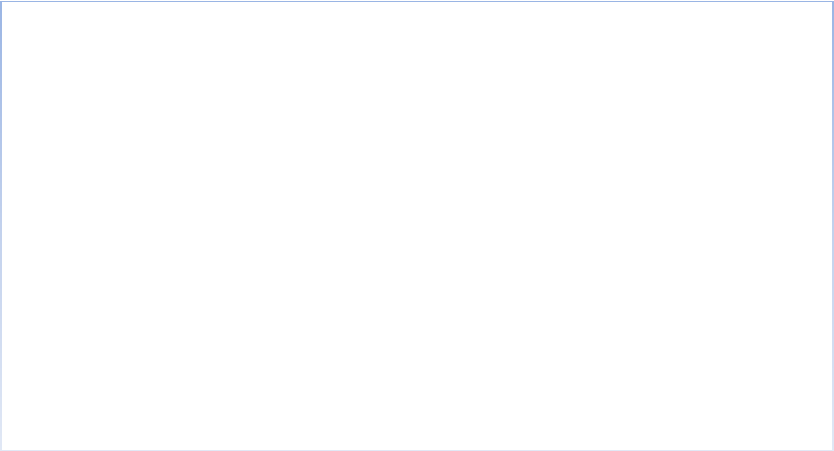
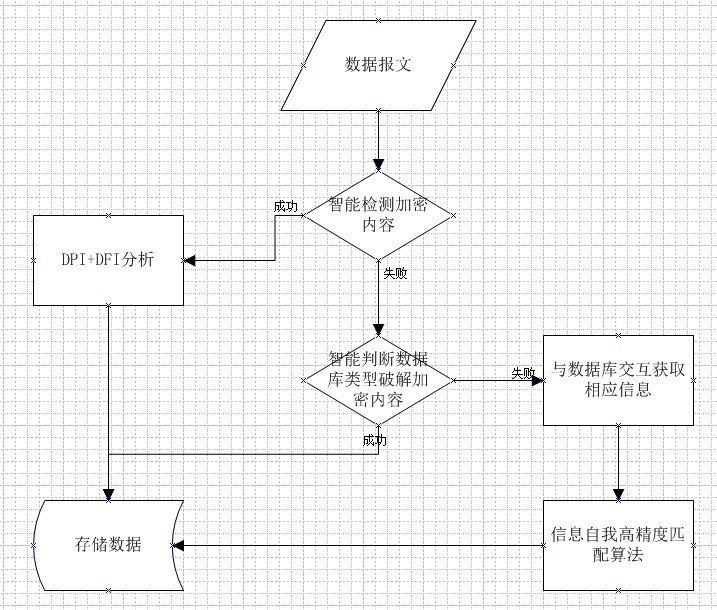
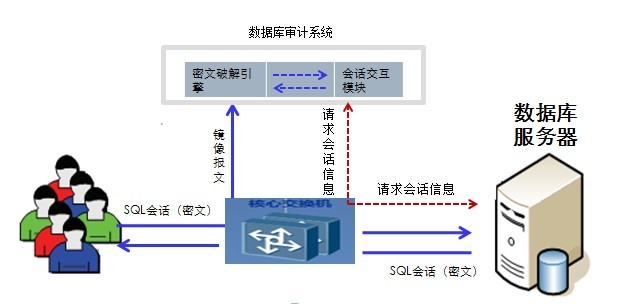


图5.2身份加密报文破译流程

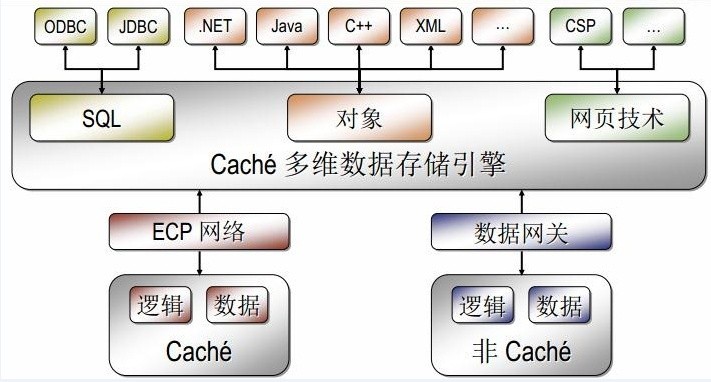


加密内容的破解在缺少密钥及加密算法支持的情况下是一个很费时又费资源的过程，在网 络实时性要求较高的审计环境中，在不影响数据库审计系统自身性能及对应用系统数据库服务 器很少影响的情况下，实现对加密身份信息的破解及提取，无疑不是一个很好的方法。

## 5.5 首创后关系型数据库的审计

目前国内外应用最广、市场推广价值更高的后关系型数据库莫过于CACHE数 据库，该数据库在国外大型医疗机构使用较广，在国内大型三甲医院及区域医疗项 目中也多有应用，如：南山区域医疗项目中使用的就是CACHE数据，CACHE数据 库因其本身使用的技术及存储结构的不同，其查询性能比市场占有率最高的 ORACLE数据库要快几十倍。

Cache数据库使用的关键数据结构为Global字典，区别于传统的关系型数据 库，同时CACHE数据库支持普通SQL命令访问，也支持面向对象的访问同时还支 持M（多语言）访问技术，数据结构如下：



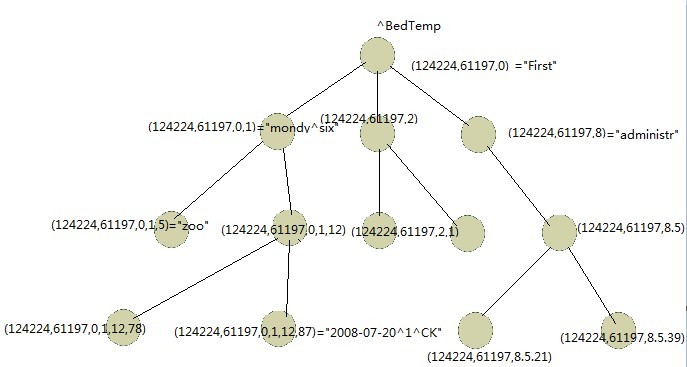


图5.3CACHE数据库的结构示意图

网神SecFox首创后关系型数据库审计技术



CACHE数据库打破了传统的关系型数据库的束缚，在国内多家大型医院成功应用后大有替 换oracle数据库成为医疗行业的首选数据库之势，CACHE数据库是医疗信息化过程中一个不可 多得的选择，目前北京妇幼保健院、四川省妇幼保健院、山东省立医院、南山区域医疗等大型 医疗机构使用了CACHE数据库。

## 5.4 大数据安全监控行业领先

Hadoop是目前大数据使用最广泛的框架之一,其数据库HBASE是采用分布式 文件系统核心技术的新型NOSQL数据库,也是俗称的大数据数据库。该数据库有丰 富的SQL及NOSQL工具及对外开放的软件接口，就像cache数据库需要全面进行 监控审计。

HBase数据库的基本架构是：

**底层**：存储层，文件系统HDFS；

**中间层**：资源及数据管理层，HBASE、YARN以及Sentry等；

**上层**：MapReduce、Impala、Spark等计算引擎； **顶层**：基于MapReduce、Spark等计算引擎的高级封装及工具，如

Hive、Pig、Mahout等。

该数据结构如下：



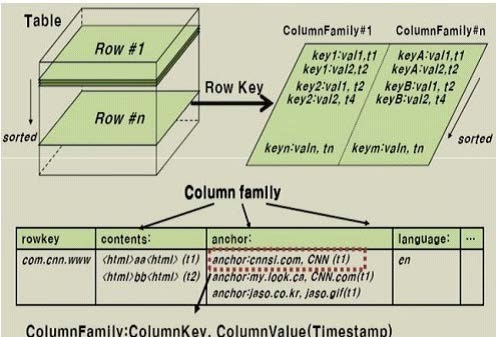


图5.4Hbase数据库同时存储结构化和非结构化数据

目前网神SecFox已经率先在行业实现了对其SQL及NOSQL的安全监控。



Hadoop是目前大数据使用最广泛的框架之一,而大数据是市场的最大趋势之一。在国内政

府，各大行业都是部署的大数据平台，网神大数据数据库审计是一个不可多得的选择。 Hadoop环境下对HIVE工具的审计 HIVE是基于Hadoop的一个数据仓库工具，多用于数据仓 库的统计和分析。 网神能审计到具体的操作行为，清晰直观。

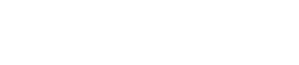
## 5.5 首创工业控制实时数据库的安全监控

工控数据库是连通生产计划调度系统（ERP、MES等）和实时生产控制系统

（SCADA、DCS、PLC等）的关键数据库，一般都是NOSQL数据库。

ERP、MES等系统使用的是传统关系型数据库，如ORACLE等。大系统的数据 库都至关重要，如果被攻陷，将会直接影响正常生产！

该数据结构如下：



**企业管理（ERP）**

**生产执行系统（MES）** **监视与人机接口(SCADA)**

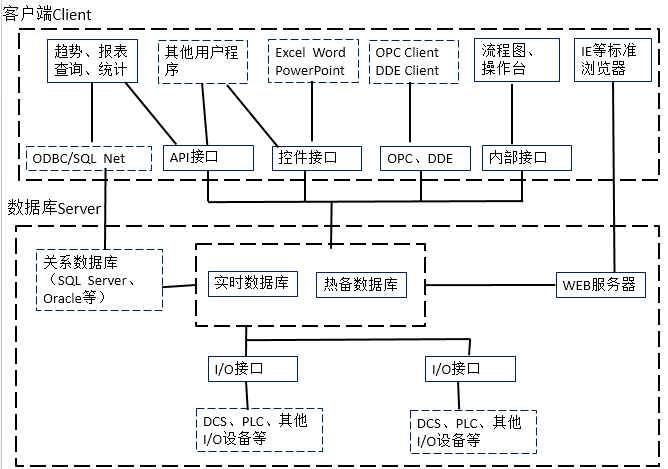
**单元控制**

**回路控制**

**传感器、变送器、执行器**

**被控主设备**

工业控制信息化系 统架构示意图

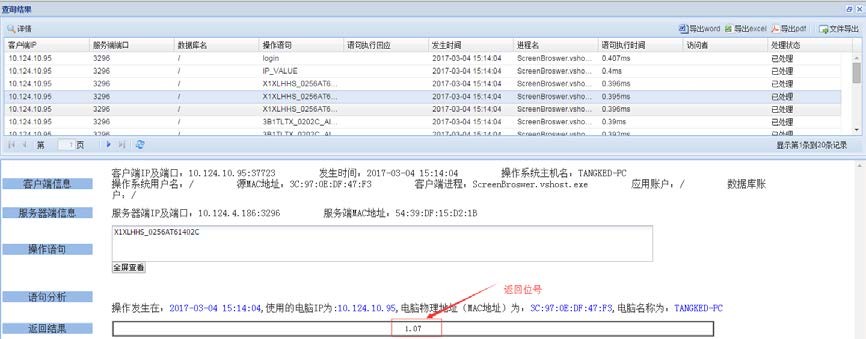


5.5工业控制数据库接口拓扑示意图

网神SecFox工业控制数据库审计系统在行业内首创对典型数据库IP21的监 控，一台设备可同时监控两大系统的不同类型的数据库，保障生产的顺利进行。



工控数据库是连通生产计划调度系统（ERP、MES等）和实时生产控制系统（SCADA、 DCS、PLC等）的关键数据库，一般都是NOSQL数据库。目前大多数工厂和一些大型的企业都 是用的该数据库。工控实时数据库IP21的审计，IP21通常有WEB和API调用等方式进行操作。 而 网神能审计到WEB操作指令及API调研用的指令。审计效果如下图：



# 6 产品资质

 公安部计算机信息系统安全专用产品销售许可证

 中国国家信息安全产品认证证书

 国家保密局涉密信息系统产品检测证书

 国家版权局计算机软件著作权登记证书

 中国国家信息技术产品安全测评证书

 军用信息安全产品认证证书