www.legendsec.com

# 网神SecFox-NBA
# 网络安全审计系统（数据库审计）

SecFox-NBA安全审计系统（数据库审计）采用旁路侦听的方式对内部用户连接到重要业务系统（服务器、数据库、业务中间件、数据文件等）的数据流进行采集、分析和识别，实时监视用户访问业务系统的状态，记录各种访问行为，发现并及时制止用户的误操作、违规访问或者可疑行为。

## 需求分析

由于政府和企事业单位的数据库系统都实现了网络化访问，内部用户可以方便地利用内部网络通过各种通讯协议进行刺探，获取、删除或者篡改重要的数据和信息。同时，一些内部授权用户由于对系统不熟悉而导致的误操作也时常给数据库系统造成难以恢复的损失。

另一方面，为了保护敏感信息、加强内控，国家强制机关和行业的主管部门相继颁布了各种保护公民隐私，以及合规和内控方面的法律法规和指引。其中《**中华人民共和国刑法（七）》第253条明确规定“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。”**

## 产品介绍

### 全面保障核心业务和关键数据

SecFox-NBA数据库审计系统能够对复杂网络环境下的各种数据库操作行为进行细粒度审计。具备独有面向业务的安全审计技术，通过业务网络拓扑记录客户业务网络中各种数据库、主机、web应用系统相互的关联性，审计人员可以根据业务网络的变化快速查看业务网络中各个设备和整个业务网络的事件和告警信息。SecFox-NBA为客户提供了丰富的报表，使得管理人员能够从各个角度对业务系统的安全状况进行审计。

## 产品亮点

- **基于旁路侦听的工作原理和灵活便捷的部署方式：**

  SecFox-NBA数据库审计系统采用旁路侦听的方式进行工作，对业务网络中的数据包进行应用层协议分析和审计，就像真实世界的摄像机。部署十分方便，即插即用，不必对业务网络结构做任何更改，对业务网络没有任何影响。

- **细粒度数据库行为审计、操作回放：**

  SecFox-NBA数据库审计系统能够对多种操作系统平台下各个版本的SQL Server、Oracle、DB2、Sybase、MySQL 、Informix、达梦等国内外知名数据库及定制数据库进行审计。审计的行为包括DDL、DML、DCL，以及其它操作等行为。

- **可视化的业务审计：**

  SecFox-NBA数据库审计系统为用户提供了简介易用的操作界面，使得普通管理员就能够对复杂的业务系统进行审计。系统提供了多种可视化的审计手段。

网神 SECWORLD

## 功能列表

| 功能点 | 说明 |
|---|---|
| 型号 | 网神SecFox-NBA |
| 网络接口 | 4个10/100/100Base-T口,最大可扩展至10个。 |
| 数据库及业务服务审计范围 | 支持对包括MS SQL Server、Oracle、DB2、Sybase、MySQL、Informix、达梦在内的多种数据库，包括Windows、Unix、Linux、AIX在内的各种操作系统，包括WebShpere、WebLogic在内的中间件，以及VNC、FTP、HTTP、SMTP、POP3、NETBIOS、TELNET、Web Service等各种网络通讯和数据访问协议进行审计。 |
| 数据库操作记录审计 | 可审计数据库的DDL（数据定义语言）：例如Create、Alter、Drop等；DML（数据操纵语言）：例如insert、delete、update、select等；DCL（数据控制语言）：例如特权帐户执行的grant、deny、revoke等操作；以及其它操作：例如事务处理操作、备份恢复操作、执行系统或者自定义存储过程等）。审计内容可以细化到域、模式、库、表、视图、记录、字段、用户、存储过程、函数、绑定变量。 |
| 数据库返回记录审计 | 系统能够记录数据操作请求的返回结果，包括成功和失败。如果返回失败信息，则还能记录错误码。 |
| 数据库敏感信息隐藏 | 系统能够在审计员进行操作查询分析的时候隐藏敏感信息，例如涉及公司机密的重要字段对应的数值，避免因为安全审计本身出现信息泄露。 |
| 业务审计 | 管理员可以根据实际网络情况定义多个业务，并建立可视化的业务拓扑视图，快速查看业务网络中各个设备和整个业务网络的事件和告警信息。用户对业务拓扑进行编辑、拖放、连接等操作。 |
| 操作回放 | 系统能够对记录下来的数据库操作及其返回结果以会话为单位进行回放。回放的时候能够显示当前会话的源、目的地址以及会话持续的时长。 |
| 实时统计 | 可以通过实时统计功能清楚看到业务网内部告警事件、活动会话、活动会话的事件列表、被保护对象的访问情况，统计最近10分钟的数据。 |
| 事件查询 | 事件查询为用户提供了历史事件查询的手段，用户可以指定复杂的查询条件，快速检索到需要的事件信息，从而协助管理员进行计算机取证分析，收集外部访问或者内部违规的证据。 |
| 告警与响应管理 | 告警规则包括系统预定义规则和用户自定义规则两大类，用户在制定规则的时候，既可以设定审计的触发条件，也可以设定触发审计后的自动响应动作，告警后可进行发送邮件、SNMP Trap、执行程序脚本、设备联动等响应动作。系统可以直接阻断可疑的网络通讯。 |
| 审计报表 | 内置大量报表报告，包括数据库报表、FTP报表、主机报表、综合报表，等。生成的报表图文并茂，报表可以按组管理可以对报表生成进行日程规划，提供打印、导出以及邮件送达等服务，并根据计划归档报告，归档之后发送邮件通知。 |
| 权限管理 | 采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义，从而达到对每一台设备、每一项功能进行操作的控制粒度。 |
| 性能指标 | 运行平台:WINDOWS、Linux、HP-UX、Solaris及AIX<br>事件处理性能：24000条/秒（TPS，Transactions per Second）<br>本地存储：3TB热插拔硬盘，支持外接存储设备。<br>浏览器并发连接数：50个（即同一时刻可以有50个用户使用本系统）。<br>用户使用模式：无需安装客户端，使用IE浏览器访问管理中心。 |
| 其他 | 部署方式：可以独立部署，也可以级联部署、分布部署，还可以与LAS、UMS集成。 |

网神 SECWORLD

欲获取更多信息，请即联系网神信息技术（北京）股份有限公司
全国统一热线服务电话： 400-610-8220（7×24小时）
E-mail：service@legendsec.com
网站地址：www.legendsec.com

传真：010-62972896
通信地址：北京市海淀区上地信息产业基地开拓路7号
先锋大厦2段1层 (100085)