



天玥网络安全审计系统 V6.0

天玥网络安全审计系统 V6.0 是启明星辰集多年网络安全产品研发经验，自主研发推出的一款针对业务环境下的网络操作行为进行细粒度审计的合规性管理系统。它通过对业务人员访问系统的行为进行解析、分析、记录、汇报，用来帮助用户事前规划预防，事中实时监视、违规行为响应，事后合规报告、事故追踪溯源，同时加强内外部网络行为监管、促进核心资产（文件服务器、邮件服务器、数据库服务器等）的正常运营。对于业务系统的核心系统审计能力表现尤其出色，是解析粒度最细的审计产品。

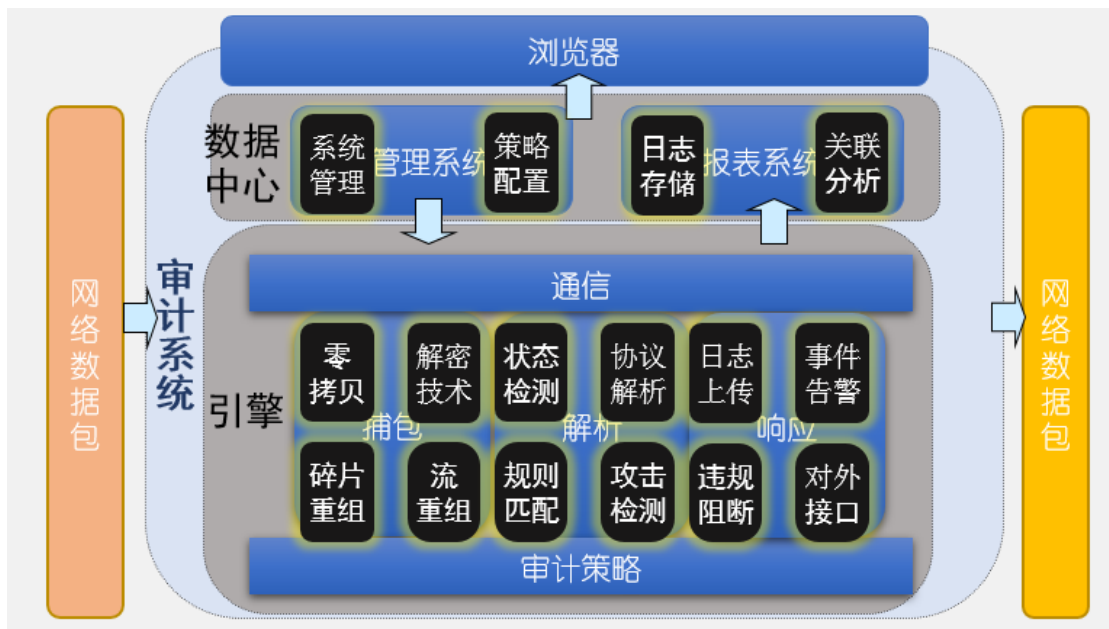


（仅供参考，请以实际供货设备为准）



一、系统结构

审计系统软件结构由引擎、审计数据中心两部分组成，如下图所示：



(1) 数据中心

B/S 架构，负责系统管理、策略配置、日志存储与关联分析。通过把配置好的策略下发给引擎，指导引擎对匹配特定策略的数据流量进行解析，同时接收并存储引擎上报的日志，进行进一步的分析与展示。系统内置存储，可存储审计日志供用户查询和分析，并可根据用户要求生成各种格式的审计报表。

(2) 审计引擎

系统审计引擎旁路接入到用户业务网络，捕获网络访问流量，根据用户配发的审计策略，对网络数据包进行深入解析，提取审计事件并进行响应。审计引擎的工作基础为审计策略，设备内置捕包、解析、响应模块，捕包模块负责对网络数据包进行捕获和重组，并根据预置的审计范围进行初步过滤，为后续解析做好准备；解析模块利用状态检测、协议解析等技术，对网络数据库包进行分类过滤和解析，然后依据审计规则对重要事件和会话的进行审计，同时也会检测数据包是否携带关键攻击特征。审计事件、会话和攻击均会提交至响应模块，响应模块负责根据审计策略对此进行响应，包括将审计日志上传至数据中心进行存储、发送事件到实时告警界面进行告警、对关键威胁操作进行阻断，也能通过邮件、Syslog、SNMP 信息的方式将审计日志发送给其他外部系统。





二、产品特点

➤ 全面的审计协议支持

审计系统能够对数据库类协议、运维类协议、邮件类协议和互联网类等协议进行审计。

系统不单单对于互联网类协议（HTTP、HTTPS）、运维类协议（Telnet FTP、Netbios Rlogin）邮件类协议（POP3、SMTP）进行审计，对于主流的数据库，例如商业数据库（Oracle、SQL Server、Informix、DB2、Sybase）、行业数据库（Teradata、Cache）、开源数据库（MySQL、PostgreSQL）、国产数据库（人大金仓、达梦、南大通用等），以及近几年来兴起的 Nosql 型数据库（MongoDB、Redis）和大数据架构下的数据库（Hive、HBase 等）均能够有效解析和审计。

➤ 灵活而丰富的策略配置功能

审计系统依据 RBAC 模型，提供了灵活而丰富的策略配置功能，协助用户完成审计策略的精确定义。审计策略可根据审计源（源 IP 地址、资源账号）、时间（即策略生效时间，可以是某一固定时间，也可以是某个周期性时间）、规则集（定义需要被审计的操作集合）、响应方式（包括事件风险级别、是否告警等）等要素来定义。

➤ 关键表、命令及字段智能分析

审计系统能够根据审计协议的类型进行命令和字段的自动提取，用户可以选择提取后的命令或字段作为重点对象进行分析。针对数据库类协议，可分析并形成数据库名、表名、命令等列表；针对运维类协议，可分析并形成命令等列表；针对文件操作类协议，可分析并形成文件名、操作命令等列表。通过该智能分析功能，可以简化用户对审计数据的分析过程，提高分析效率。





三、产品功能

功能项	功能描述
用途说明	能够分析和详细记录应用和各类工具对数据库的访问行为，对数据库资源违规访问进行告警。
协议支持	支持国产达梦，人大金仓、南大通用、神舟通用、高斯数据库，支持国外 Oracle、SQL Server、Sybase、DB2、Informix、mysql 等数据库；能够分析不同应用访问数据库的方式、行为和主要特征。并根据特征进行数据库访问语句优化。
策略定义	数据库审计策略支持操作命令、数据库客户端软件名称、数据库名、数据库表名、数据库返回码、字段名称和字段值作为分项响应条件（非正则表达式方式）。
细粒度审计	支持记录数据库操作的源/目的 ip、源/目的端口、源/目的 MAC、重定向端口、资源账号、命令、表名、sql 语句、客户端程序、连接方式、客户端用户、源主机名、目的主机名、子命令、响应时间、影响行数、错误码、数据库名等。
操作展示	支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源 ip、客户端程序名、业务操作、错误码、表名等按需定义，可根据昨天、最近七天、最近 30 天以及自定义时间并且可精确到小时进行轨迹显示，可显示下一节点数量，维度可排序，可在某一维度中进行筛选。
敏感信息掩码	支持敏感信息掩码，用户可以针对姓名、身份证号、手机号、银行卡号、住址以及自定义信息进行敏感信息掩码配置，姓名、身份证号、手机号出厂有默认的掩码配置，无需配置，方便使用，防止敏感信息在审计系统中进行泄露。
审计报表	提供缺省报表模板，包括 SOX 报表、PCI 报表等模板，供用户选择使用；支持用户自定义报表模板，包括数据集、图表设计、数据设计等，数据设计可根据不同数据集提供不同的分析维度和指标供用户进行选择；支持按每天、每周、每月、手动指定某一时刻生成报表，生成的报表支持邮件方式自动发送；支持生成 Word、PDF、xls、HTML、WPS 格式的报表导出，支持报表的自动邮件发送。
审计查询	具备审计查询功能，对于数据库访问日志，支持按源目的 ip、源目的端口、源目的 mac、级别、客户端程序名、数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、SQL 语句关键字、数据库返回码、SQL 响应时间、数据库返回行数作为查询条件；可支持根据 sql 语句关键字进行查询，查询事件为 sql 语句中包含该关键字的所有符合条件的操作记录；查询需返回全部符合查询条件的事件，不可限制最大返回数量。
自动发现	支持用户环境中的数据库和资源账号、表名的自动发现，其中资源账号发现支持资源账号、在线天数、发现日期等信息；表名发现支持表名、数据库名、发现次数等信息；数据库服务器发现支持数据库协议、IP 地址、端口、识别时间等信息。





异常场景分析	支持基于场景的操作异常分析；可直观展现数据库异常、上下班操作量对比异常、疑似暴力破解、疑似撞库攻击、访问时长审计、还有账号多 IP 登录是否要加入。
一键自检	支持一键自检功能，可以检查系统当前运行状态，检查内容包括：系统信息、进程信息、数据库信息、授权信息、用户信息等 17 项内容，协助管理员迅速定位系统异常，减少日常维护工作量。
自身管理与维护	提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。
自主可控	采用国产飞腾 CPU 处理器、银河麒麟操作系统。
接口规范	产品支持 GCB010-2017《安全管理接口技术要求》、GCB007-2017《安全审计服务规范》或以上版本的相关要求进行相关适配工作。
技术资料	用户手册包含产品介绍、产品组成、工作原理及过程、安装/卸载、操作指南、常见故障及处置、服务提供。
	光盘 1 张，含完整用户手册。
配件	普通直连网线 1 根，电源线 2 根，串口线 1 根。





四、产品规格

产品型号	CA-FT-3000UR-ZFA
产品形态	标准 19 英寸机架式设备
日处理事件数	1.5 亿条
Sql 解析能力	3 万条/秒
尺寸（长*宽*高）	560mm*435mm*88mm
网络接口	2 个千兆电口，4 个万兆光口（含单模模块）
扩展槽位数量	3 个扩展槽位
USB	2 个
Console 口	1 个
工作温度	5℃~35℃
存储温度	-20℃~60℃
工作相对湿度	20%~80%
电源	220V±22V；50Hz±2Hz
	冗余电源

