昂楷科技

昂楷数据库多重审计系统

后关系型数据库，安全监控的首创者、唯一全面支持者

InterSystems

CACHE

Post-Relational Database

目录 CONTENTS

公司简介

使命

让人们放心地享受大数据

愿景

成为顶级的数据安全治理领导者

价值观

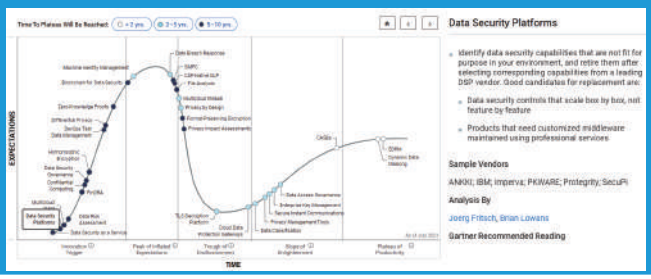
踏踏实实做人，扎扎实实做产品，不做“关系型”产品

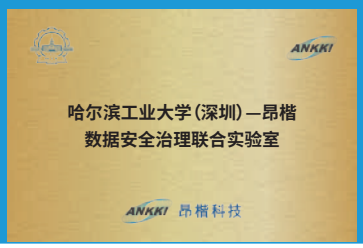
深圳昂楷科技有限公司是领先的数据安全治理产品及解决方案专业研发企业，从公司成立伊始，就聚焦于数据安全领域。已经为医疗、政府、公检法司、电信运营商、电力、石化、互联网、先进制造等多个行业的3000多家客户提供了数据安全解决方案。产品解决方案广泛适用于大数据、云计算、云原生、人工智能、工业控制、物联网、智慧应用、IDC等应用场景，形成了完整的结构化SQL及NoSQL数据安全解决方案体系，涵盖DCAP、DAP、DSP等领域。产品解决方案及服务有：数据安全综合治理平台、数据分类分级、数据库审计、数据库防火墙、数据脱敏、数据库漏扫、数据库状态监控、数据水印、集中管理平台和数据安全风险评估、数据库渗透测试服务等，构建了数据资产运营、行为模型运营、安全风险运营和安全策略运营四维形成运营度量“五位一体”的数据安全运营体系，为客户提供全方位的数据安全治理服务。

公司秉承“为客户创造价值是公司唯一存在理由”的经营方针，狠抓“踏踏实实做人，扎扎实实做产品”的服务理念，以“不做关系型产品”为座右铭，以IPD流程为经营服务理念的落地保障；始终坚持自主研发、大力投入研发，以市场需求为导向，在数字化的浪潮里，走在行业的最前沿。

荣誉资质

- 高新技术企业证书
- 涉密信息系统产品检测证书
- IPv6 Ready Logo 认证证书
- ISO9001质量管理体系认证证书
- ISCCC中国国家信息安全产品认证证书
- 2018年贵阳大数据攻防演练“安全防卫奖”
- 2017贵阳大数据及网络安全攻防演练活动
- ISO/IEC27001信息安全管理体系认证证书
- 哈工大（深圳）-昂楷数据安全联合实验室
- 昂楷数据安全综合治理平台入选Gartner《2021数据安全技术成熟度曲线》DSP中的 亚太地区唯一推荐厂商




ANKKI
哈尔滨工业大学(深圳)—昂楷
数据安全治理联合实验室
ANKKI 昂楷科技


安全防卫奖


质量管理体系
国际标准认证证书

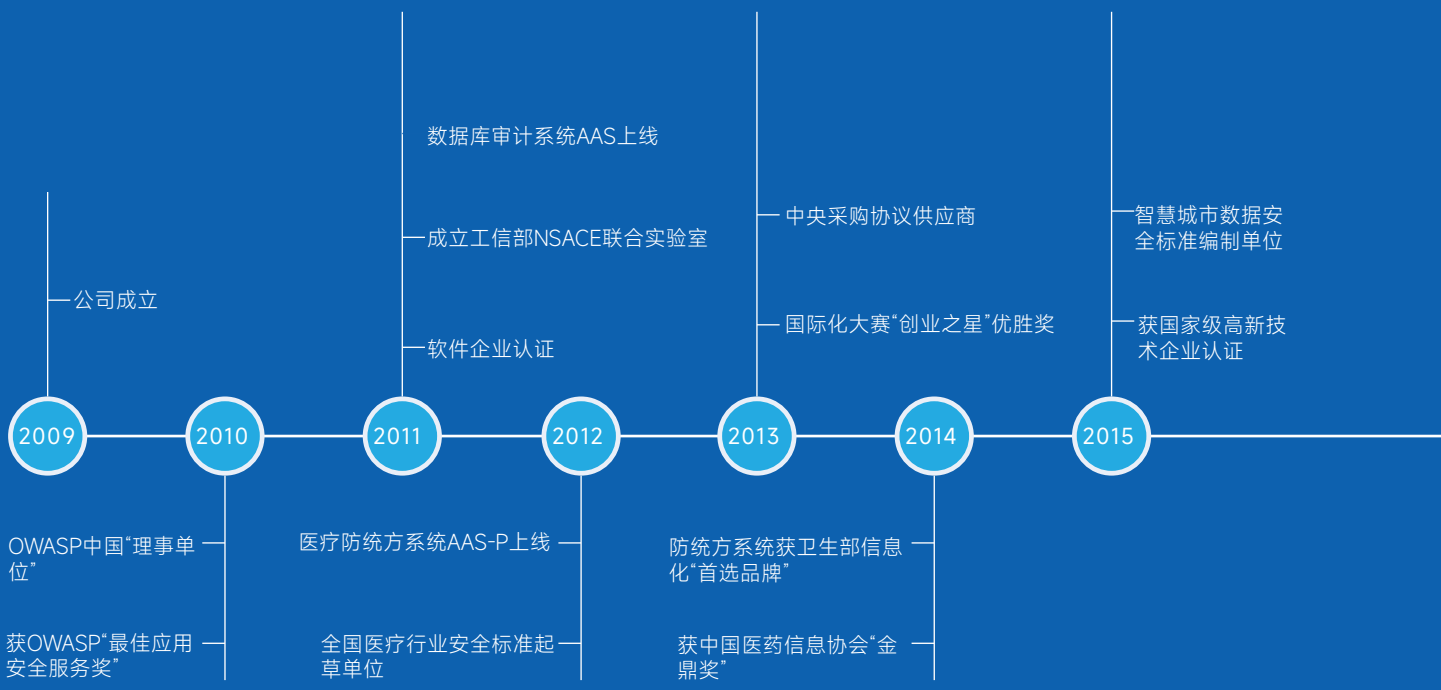

IPv6 Ready Logo 认证


中国国家信息安全产品认证证书
中国信息安全认证中心


BIGDATA2017
2017贵阳大数据及网络安全攻防
演练活动：
安全防卫奖


高新技术企业
证书

昂楷大事记


2009
公司成立
2010
OWASP中国“理事单位”
获OWASP“最佳应用安全服务奖”
2011
数据库审计系统AAS上线
成立工信部NSACE联合实验室
软件企业认证
2012
医疗防统方系统AAS-P上线
全国医疗行业安全标准起草单位
2013
中央采购协议供应商
国际化大赛“创业之星”优胜奖
防统方系统获卫生部信息化“首选品牌”
2014
获中国医药信息协会“金鼎奖”
2015
智慧城市数据安全标准编制单位
获国家级高新技术企业认证


2016
云数据库审计系统荣获中国网安“金智奖”
涉密信息系统产品检测证书
发布数据库漏扫、数据库状态监控、数据库脱敏、数据库防火墙
发布大数据、云、工控数据库审计系统
国家工程实验室合作单位
2017
中央采购协议供应商
国家信息安全产品认证证书（ISCCC）
军用信息安全产品认证证书
荣获2017年度贵阳大数据功防演练安全防卫奖
大数据审计系统获中国网安“金智奖”
2018
荣获2018年度贵阳大数据攻防演练安全防卫奖
打造数据安全综合治理方案
中央采购协议供应商
与国际著名IT咨询公司Gartner达成战略合作
2019
唯一入选2018年度IDC中国数据安全市场创新者
入选深圳市经信委网络安全技术应用试点示范项目
荣获CMMI3级认证
荣获ISO27001认证
2020
正式发布昂楷数据安全综合治理平台
获得奇安投资公司的独家投资
昂楷数据安全综合治理平台获DAMA中国优秀产品奖
2021
数据安全综合治理平台入选Gartner《2021数据安全技术成熟度曲线》DSP中的亚太地区唯一标杆性厂商
获得方广资本新一轮投资
哈工大（深圳）-昂楷数据安全联合实验室成立
承担第四届中国国际进口博览会数据安全保障工作
2020年度广东医院信息化建设“金牌合作伙伴”
加入中国信息通信研究院发起的数据安全推进计划（DSI）
首批入选北京工业互联网数据安全专委会标准工作组成员单位
昂楷数据脱敏获DAMA中国优秀产品奖
2022
入选Gartner中国数据安全标杆厂商名录
获得奇安信战略投资

数据安全是当前面临的主要挑战

网络信息安全已经从终端安全、网络安全进入到数据安全阶段，数据安全建设应该采用最新的数据安全理论建立数据安全治理体系。

数据安全是信息安全的重灾区，是所有行业都面临的问题

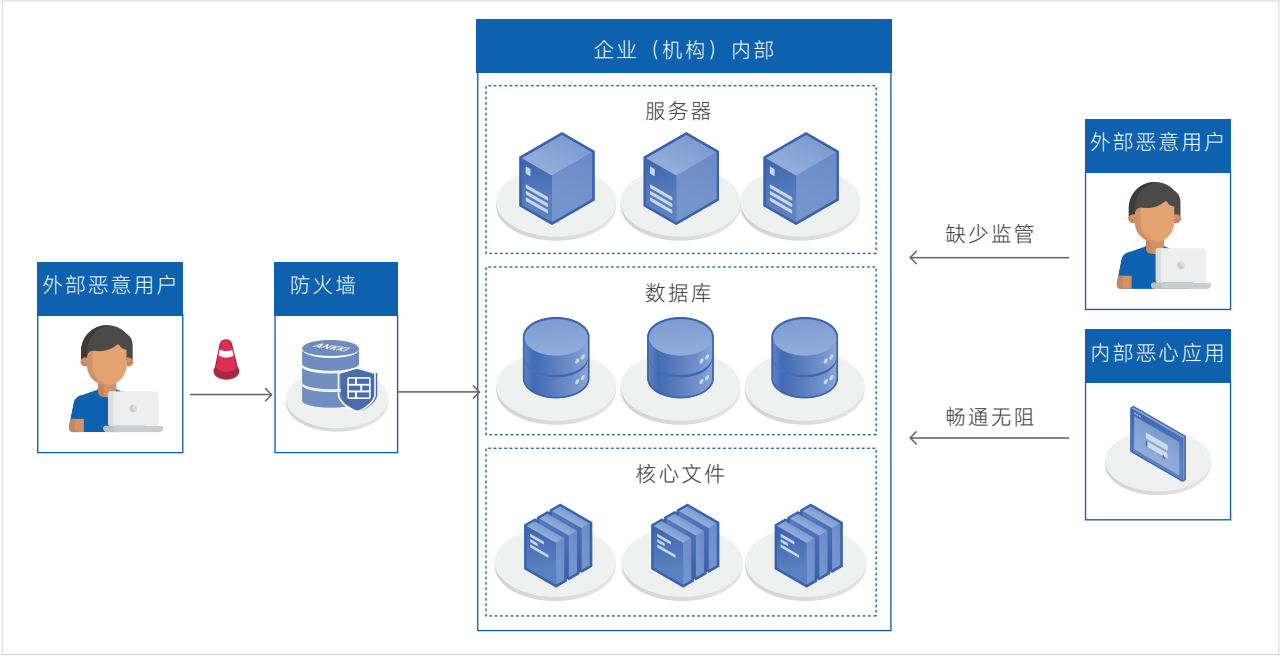
政府机构	医疗健康	金融机构	互联网
2021年3月印度政府网站泄露了数百万核酸检测结果，包含姓名、年龄、婚姻状况、检测时间、居住地址等敏感个人信息。	2020年美国医疗机构数据泄露造成130亿美元损失； 2015年2月，美国第二大健康医疗保险公司Anthem公司信息系统被攻破，将近8000万客户和员工的记录遭遇泄露。	2021年3月国内XX银行因泄露客户信息被罚450万元； 2021年1月新西兰央行数据系统遭黑客攻击或已获取商业和个人敏感信息。	2019年7月Facebook因数据泄露被罚50亿美金； 2017年3月XX大型互联网公司内部盗取涉及交通、物流、医疗、社交、银行等个人信息50亿条。

数据安全事件愈演愈烈，并且呈上升趋势

2021年05月	应用Omiai最近遭黑客攻击，约170多万用户个人数据遭泄露。
2021年04月	苹果代工厂「广达」MacBook Pro设计图纸被黑客窃取。
2021年03月	数据分析公司Polecat遭重大安全事件，近30TB业务数据被破坏。
2021年02月	Clubhouse音频数据遭黑客窃取。
2021年01月	日产公司近20GB源代码遭到泄露。
2020年12月	国内知名招聘网站泄露大量个人简历被转手买卖。

安全事件揭示的重要问题

- 信息化建设与安全保障系统没有同步；
- 投入终端及网络的“外防”多，内部核心系统及数据的“内控”少；
- 数据安全是当前最主要的矛盾。



80%安全事件都是“内部”人员所为

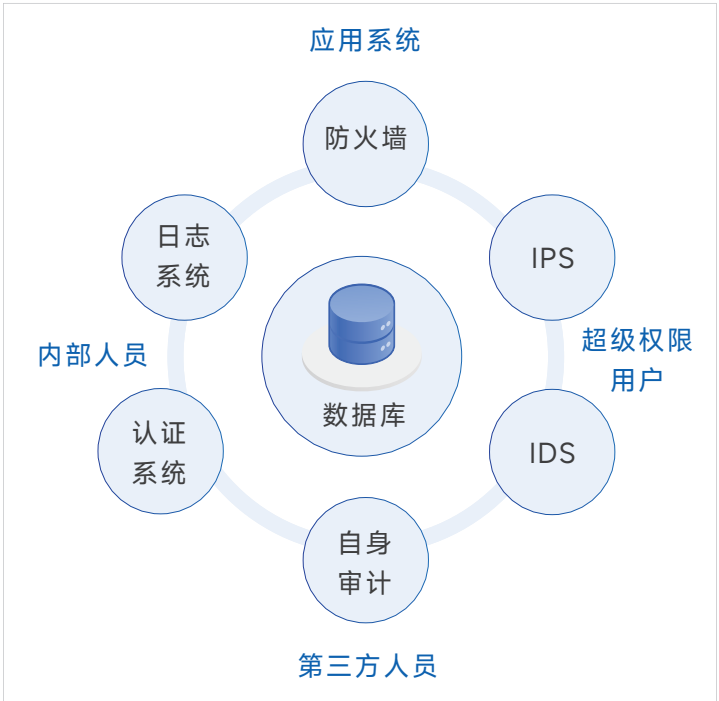
为什么需要数据库审计

数据库是重点保护对象

各行各业的业务数据几乎都存储在数据库中，数据库安全是直接针对数据主要载体进行防护的，是数据安全时代的核心需求。

- 数据库是各种信息的集散地（办公、财务、人力、物资等各种业务）。
- 数据库处于组织网络信息安全防御中心，是“兵家必争之地”。

传统手段防护能力不足，数据库危机四伏



数据库日志：
影响数据库性能，易被篡改，一般不开启；

应用系统自身审计：
对绕过APP、直接访问数据库的最危险行为却无法监控；

堡垒机：
通过业务系统等非运维类型的数据库访问行为无从监控；

日志审计：
无法做到语义识别、不能实时在线对数据库行为做分析；

身份认证、防火墙：
可将未授权人员阻挡在门外，但对合法身份访问者无法监控。

数据库安全解决方案虽多，但有效的少

非审计方案的缺陷	数据库审计的价值
◐ 需与数据库服务器发生交互，对业务产生影响； ◐ 实施周期长，需要大量人工长期参与； ◐ 投入大，收效不明显，常规攻击无法防范； ◐ 个别服务商向客户贸然推荐尚处于行业实验室阶段的产品或功能，导致常规业务大受影响，甚至损失严重。	◐ 最经济、最贴身、最有效的数据保镖； ◐ 行业认为，云计算平台下，可能是唯一的解决手段； ◐ 信息化深化建设的必然选择。

政策标准、法律法规的要求

ISO/IEC 27001对数据库主机审计的要求

01	应产生记录用户活动、意外和信息安全事件的日志，并按照约定的期限进行保留，以支持将来的调查和访问控制监视
02	记录日期、时间和关键事件的细节
03	记录成功的和被拒绝的数据以及其他资源尝试访问的记录
04	访问控制系统引发的警报
05	审计日志包含闯入和秘密人员的数据，应采取适当的隐私保护措施
06	定期评审监视活动的结果
07	系统警报或故障
08	应保护日志设施和日志信息免受破坏和未授权的访问
09	防止信息泄漏的机会
10	应收集、保留证据，并以符合法律规定的形式提交

《信息安全等级保护测评》对数据库主机审计的要求

01 审计的选择要求和策略，审计日志的保护措施。

02 为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表。

03 审计范围覆盖到每个用户。

04 对特定事件指定实时报警方式（如声音、Email、短信等）定义了审计跟踪极限的阈值。

05 跟踪监测到可能的安全侵害事件。

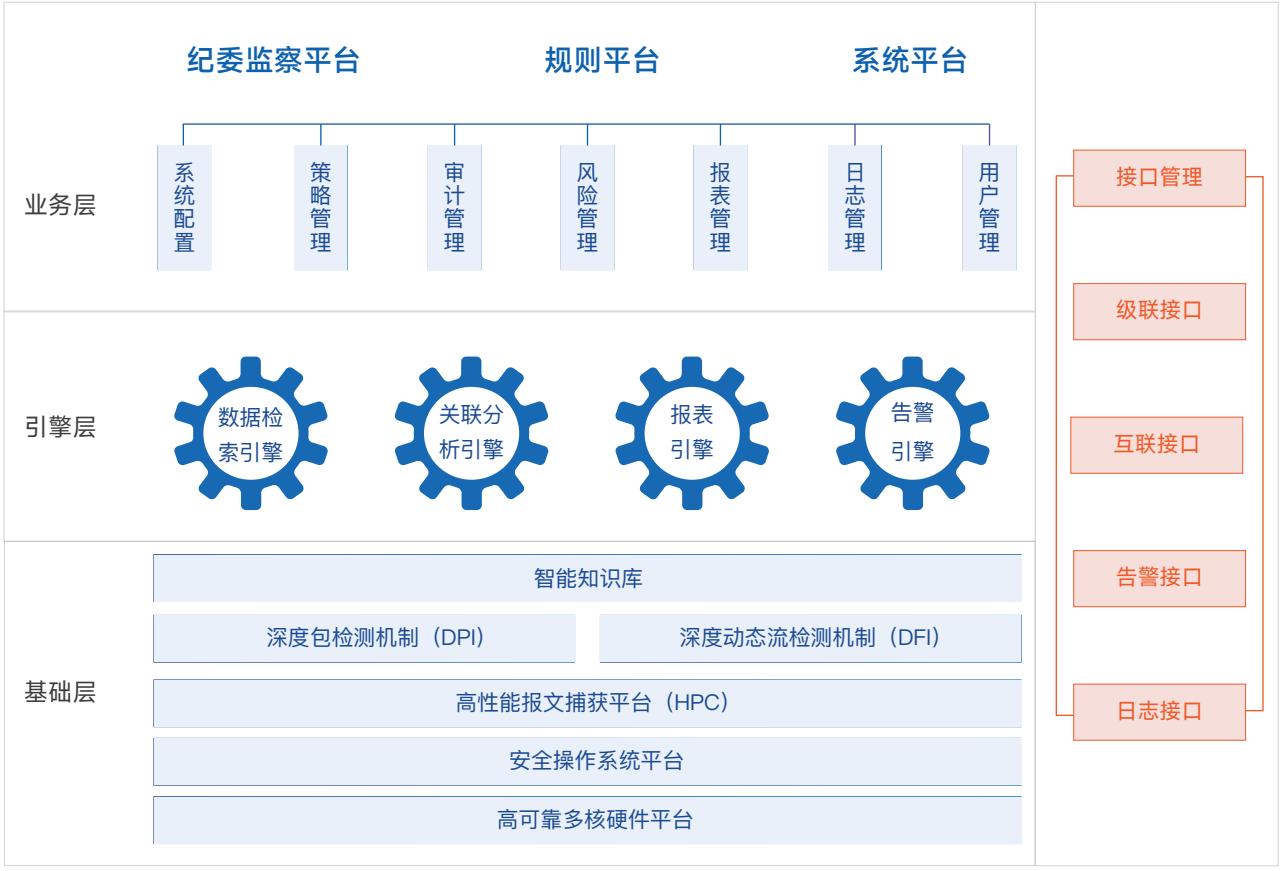
昂楷数据库审计简介

昂楷数据库审计是一款软硬一体化产品，首创双向审计机制，全面覆盖应用、中间件、数据库，达到“事前预防 + 事中防范 + 事后取证”的立体防御效果。审计系统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种操作，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，有效支持电子取证。

昂楷数据库审计总体架构

昂楷数据库审计由基础层、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”。

高价购置的专业高性能发包测试仪器，是电信级品质的保证。



昂楷数据库审计功能

审计管理平台

- 独立的审计管理平台，敏感信息自动屏蔽，告警信息智能翻译，直观可视；
- 审计管理平台采用 B/S 架构，无需安装客户端，所有功能模块，操作简单灵活，通俗易懂；
- 实时告警，当有人非法操作或者破坏设备时，系统会实时发送短信或者邮件，并作详细记录，无需24小时监控设备；
- 审计管理平台可以查询对数据库进行的所有详细操作，何时、何人、使用何种方式操作，并支持事件回溯功能；
- 审计管理平台有独立的审计日志，信息部门可以对告警数据进行查询、分析、统计、打印等；
- 提供审计管理员、规则管理员、系统管理员，实现三权分立，同时三权相互制约；
- 系统内置多种统计分析报表，源 IP 访问排行、数据库登录失败排行等。

安全管理平台

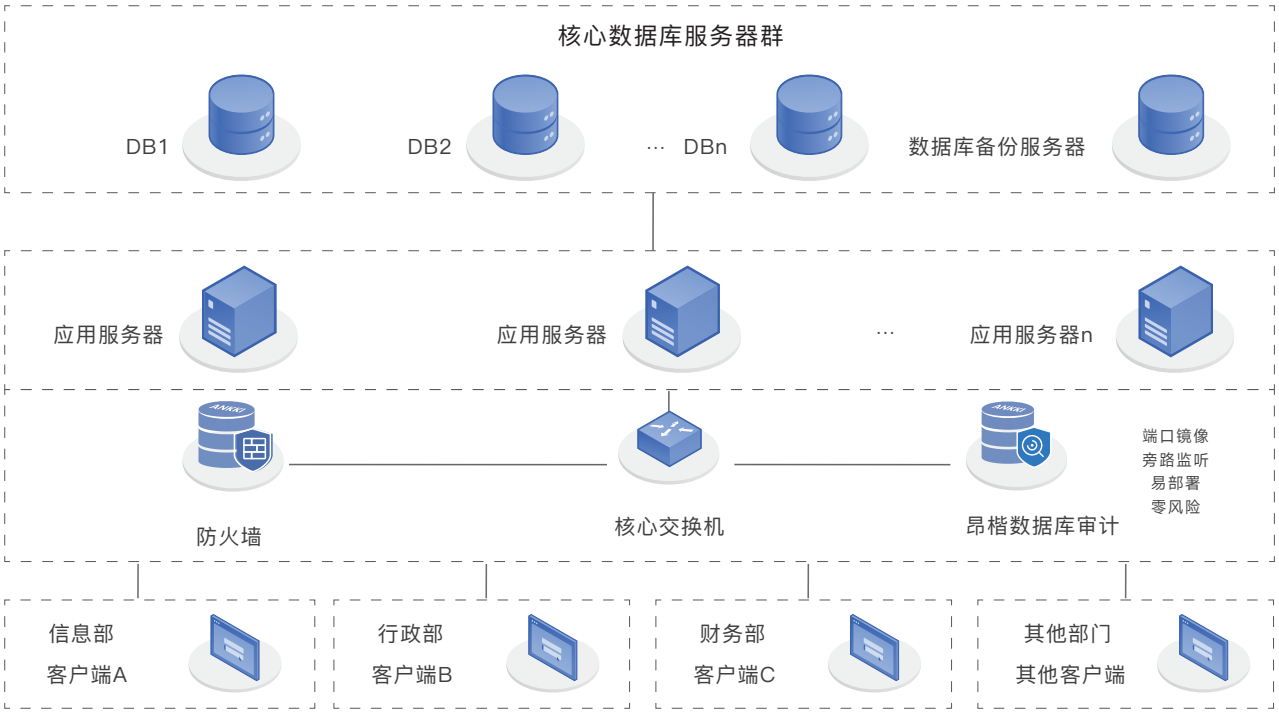
- 系统内置智能规则库，同时支持自定义规则，通过不同规则配置让系统更加符合每个企业不同的管理要求；
- 系统支持工号、源 IP、MAC、用户名、进程、操作系统类型、操作系统用户名、身份标识和审计，多重定位，杜绝仿冒；
- 系统支持数据库SSL加密流量的审计；支持SSH加密审计、SQLPlus本地审计、MySQL工具本地审计；支持对SQL Server 加密协议的审计；
- 系统支持数据库绑定变量审计，防止“高手级”黑客攻击；
- 支持大数据平台下的大数据库如：Hwi、ES、MongoDB、Impala、Spark、Hbase、Solr以及REST_API 接口审计，JDBC_API接口调用的安全审计；
- 支持传统关系型数据库，如:SQLServer、MySQL、Oracle、Sybase、DB2、Informix、PostgreSQL、MariaDB的安全审计；
- 支持国产化数据库，如：DM（达梦）、Kingbase（人大金仓）、虚谷数据库、LibrA、GaussDB、GBase、Oscar（神舟通用）的安全审计。

系统管理平台

- 自动监控数据库审计系统运行状况，当设备出现问题或者磁盘空间不足等问题时，及时通知相关负责人；
- 系统采用旁路监听方式，只分析对数据库的非法操作行为，不访问业务系统，确保对企业现有系统没有任何影响；
- 虚拟化和远程桌面审计：能够审计到详细的登录操作系统的用户名，从而区分不同的访问者；
- 系统支持分布式集中部署，通过集中监控中心将总部下辖所有单位的数据库审计系统统一管理起来；

灵活的部署方式

昂楷数据库多重审计系统是软硬件一体化的安全设备，采用自研的安全 OS 系统，内嵌数库，无需用户安装其他管理系统。



零影响

- 无需在被审计数据库服务器上安装任何软件代理或插件；
- 无需提供被审计数据库服务器的任何管理账号和密码；
- 在运行中审计产品无需访问被审计数据库，真正零交互；
- 无需重启被审计系统及服务，拒绝业务中断；
- 对原有网络不造成影响，审计产品的故障不影响业务的正常运行；
- 率先支持 IPv6 环境部署，领先同行。

开放接口

- 系统预留了接口，可作为二次开发接口，也可与上一级的系统对接；
- 高效管理区域内的数据库审计系统，分支节点不再各自为政，全部在统一监管下，有效提高区域性数据库审计的效益；
- 提升区域内各机构的数据安全整体应急能力，出现紧急情况能第一时间响应处理；
- 快速了解区域各节点数据库审计使用情况，保证数据库审计系统正常运行；
- 汇总各节点数据提供有效的报表，为管理部门制定相关信息化政策提供依据。

为什么选择昂楷数据库审计

昂楷数据库审计系统优势概览

理念先进

- 多重审计，精准防御；
- 数据库零影响，不产生任何交互；
- 多重自身安全机制（三权分立、隐秘数据，报表加密），防范二次泄密。

全方位无死角防护

平台优势

- 一库（智能知识库）、二机制 （DPI+DFI）、三平台（硬件、OS、HPC）、四引擎（数据检索、关联分析、报表、告警），构建平台优势；
- 预留接口，开放互联
- 大数据技术，支持分布式集中部署

大数据技术

技术创新

- 全面支持后关系型数据库Caché的审计，包括对其客户端工具Terminal、Portal、Studio、SQL Manager、Med Trak 的审计
- 独创 “六元组”（应用层账号、数据库账号、操作系统用户名、客户端主机名、客户端 IP、客户端 Mac） 可准确定位到人
- 支持三层模糊关联和 HTTP 协议的审计
- 支持 MS SQL Server 加密身份信息破译
- 支持多种中间件，COM、COM+、DCOM 等
- 支持绑定变量及嵌套语句的复杂组合的审计
- 支持虚拟云审计：虚拟桌面、服务器虚拟等
- 语句审计长度多达 50k
- 告警检索效率高达亿条数据秒级
- 有效解决数据库端口变换及编码变化的疑难问题
- 可监控执行时间长达 48 小时的操作
- 系统支持告警翻译，方便非技术人员独立使用

第四代产品，不误报、不漏报

昂楷数据库审计系统已率先进入第四阶段

数据库的发展经历了层次数据库、网状数据库、关系型数据库、后关系型数据库的不断演进，融合了面向对象技术和Internet网络应用技术的新一代后关系型数据库。数据库技术的改变，数据库安全审计系统要适应新的数据库的技术需要而变化。后关系型数据库的安全审计是信息安全领域崭新的课题，对于此项技术的研究，长期以来，无论是国内还是国外都还没有商用的技术产品问世，而昂楷科技以已有关系型数据库审计产品为基础，全面支持最新一代数据库的审计。

数据库审计技术的演进

第一阶段

流量行为审计

实现了对OSI七层模型中的网络层到会话层的覆盖，主要对数据库访问行为进行分析和统计。

第二阶段

内容审计阶段

实现了对OSI七层模型中的表示层到应用层的覆盖，利用关键字对SQL整个语句进行模糊匹配，主要对数据库访问行为实现内容记录，如数据库登陆账号、SQL语句等。

第三阶段

语法解析阶段

该阶段集中在应用层，实现对SQL语句的语义分析，尽可能的将操作数据库的SQL语句进行细粒度解析，比如账号名、数据库名等等。

第四阶段

后关系数据库审计阶段

解决面向对象的M语言安全审计问题，首先要识别协议，识别各种面向对象的访问方式，如Terminal、Http、Studio等，数据库的存储格式也变的多维。

昂楷数据库审计系统核心能力

全面审计

- 支持终端用户审计、双向审计；
- 支持常见SQL语句、复杂SQL语句深度审计；
- 支持国际、国内主流的关系型、非关系型数据库。

威胁防护

- 及时预警，或旁路阻断；
- 风险展示，安全指数分析；
- 常见内部用户异常行为、外部攻击识别。

高效分析

- 支持海量数据在线分析；
- 高效SQL解析引擎，高达5万条/秒；
- 提升入库和查询能力，亿级数据秒查。

精细监控

- 内置丰富报表，满足内外审要求；
- 支持18个字段配置，定义精细审计规则；
- 内置500+丰富的行业规则，方便用户使用。

支持后关系型数据库审计

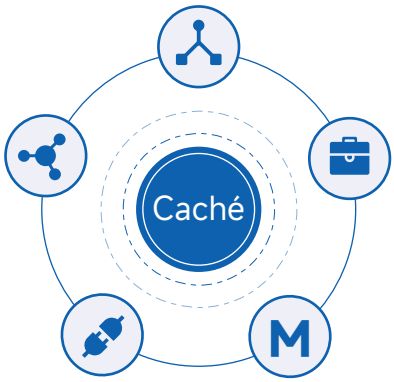
Caché正在成为高性能数据库应用场景的新宠（特别是医疗卫生行业），这是NoSQL的一个典型代表。昂楷首创了后关系型（面向对象）数据库Caché的M语言的解析和审计技术。

支持Caché数据库集成工具Terminal、Portal、Studio、SQL Manager、MedTrak工具的审计，其中Portal能审计到SQL语句、查询Global、返回结果，Terminali能审计到M语句和返回结果。

Caché数据库特点

采用树形结构
在性能上要比传统的结构型数据库高约30倍

结构化和非结构化数据并存



五种工具的使用
SQL Manager / WinSql、Studio、Portal、Terminal、MedTrak

丰富的接口类型
ODBC、JDBC、Java API等

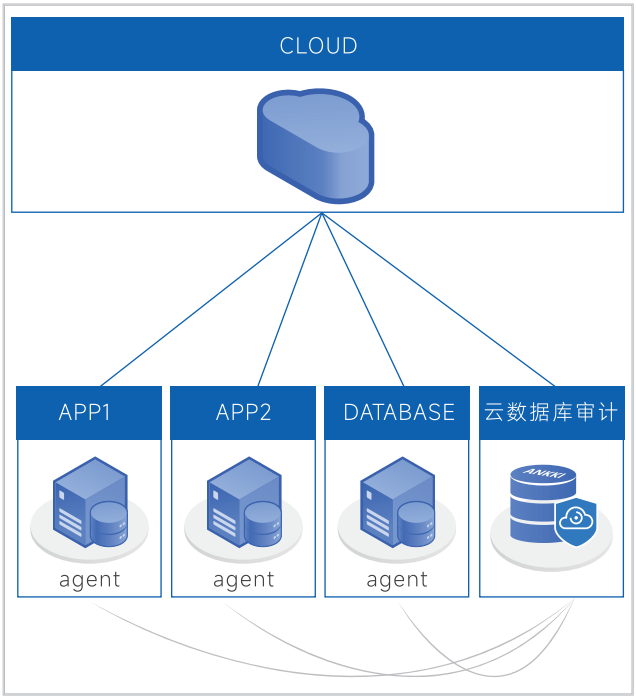
复杂的M语言
SQL只是其中一种

昂楷-Caché全面审计

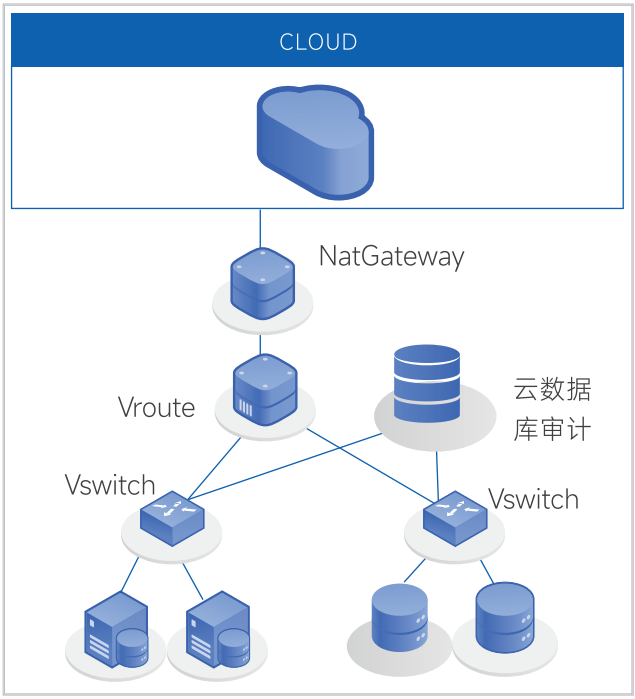
实际审计效果（以Medtrak为例）

支持云数据库审计

虚拟化环境或者云平台由于内部的虚拟交换机流量很难镜像或者无法镜像，因此传统的数据库审计解决方案不足以应对虚拟化和云平台的数据库审计需求。昂楷通过报文引流技术解决“看不到”报文的问题，率先攻克了对云平台架构的数据库审计技术。提供无插件及轻量级插件两种方案，对数据库“零”影响。



云数据库解决方案（轻量级插件）示意图



云数据库解决方案（无插件）示意图

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和NoSQL工具及对外开放的软件接口，就像Caché数据库需要全面进行监控审计。目前昂楷科技已经率先在行业实现了对其SQL及NoSQL的安全监控。

大数据安全的挑战
◐ 数据价值显著上升，对窃取、篡改、攻击行为等无法判断和拦截；
◐ 数据流转使用时，无法有效进行监控及溯源；
◐ 数据共享交换，难于保证数据的保密性；
◐ 新型大数据技术和架构成为大数据审计难题。

难点	
SQL及NoSQL共存	丰富的应用工具
接口众多且开放	采用分布式架构

大数据安全审计能力	
全面监控审计	支持传统关系型数据库，还支持HDFS、HBase、Hive、Hue、ES、Mongo等NoSQL数据库及组件操作的审计；
多类型接口审计	支持API、JDBC、REST Full API、Shell等众多接口审计，监控应用系统及开源工具访问数据库的行为；
分布式架构审计	支持对HDFS的NameNode及DataNode节点，HBASE的Hmaster及HRegionServer节点等分布式架构的流量关联审计。

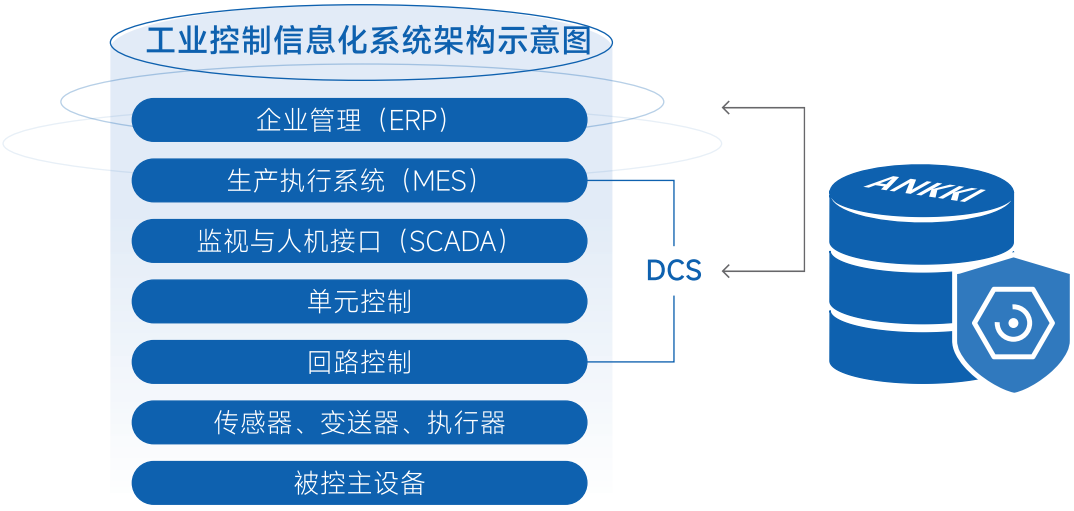
工控数据库的安全监控及审计

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。

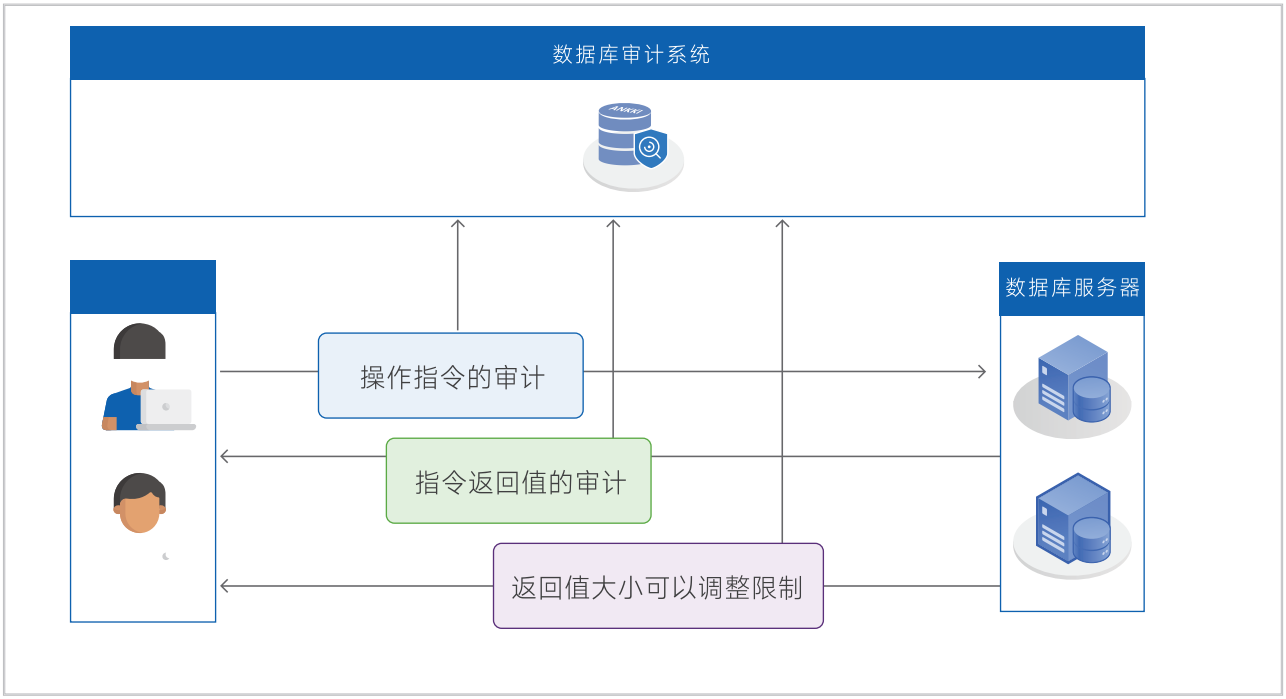
两大系统的数据库都至关重要，如果被攻陷，将会直接影响正常生产！

昂楷科技工业控制数据库审计系统在行业内首创对典型数据库P21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。



深度检测、双向审计，无漏网之鱼

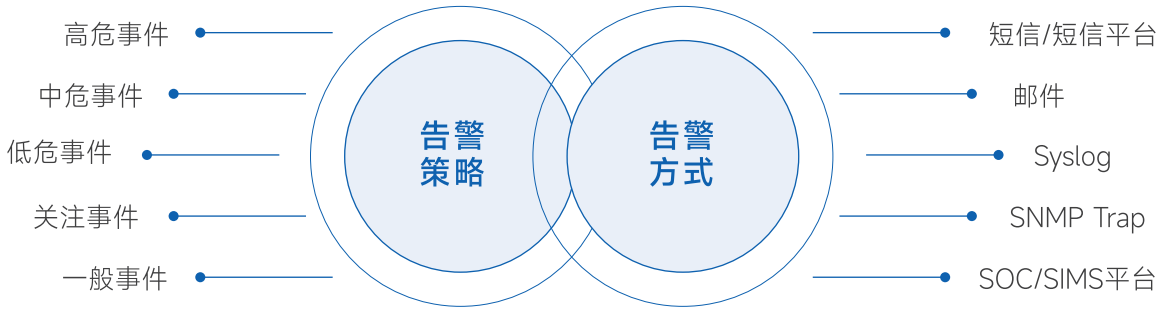
支持嵌套、函数、绑定变量、长语句、返回结果、脚本等复杂操作和隐秘操作的审计，深度识别和立体分析，不漏审、不误审，准确防范各种危险操作行为。



多种方式实时告警，智能翻译，方便非技术人员独立使用

根据不同平台、环境可适配不同的告警方式；开放式接口及多种协议支持即可实现传统告警方式，也可满足平台的对接需要

告警策略：从高危事件、中危事件、低危事件、关注事件、一般事件选择告警，同时配置告警接受者和多种通知方式。



实时告警、详细信息，可事前预防、事后取证

独创“六元组”，可真正定位到“人”

同时支持应用层帐号、数据库帐号、操作系统用户名、客户端主机名、客户端IP、客户端MAC。而行业内一般只能支持到后面的“五元组”，在复杂环境下，难以定位到人。

能够防范黑客级“高手”，让其无可遁形

有别于一般的数据库审计产品，昂楷数据库审计系统能防范绑定变量、函数等高级别的数据查询操作，善于抓“高手”。

绑定变量审计示意图

函数审计示意图

定向行为分析，取证得心应手

通过定向行为分析，可以明确出某指定客户端在某段时间内所有的操作记录，从而进行现场重建，录像回放，真实再现完整操作过程，进行电子取证，为溯源和取证提供有力的证据。

绑定变量审计示意图

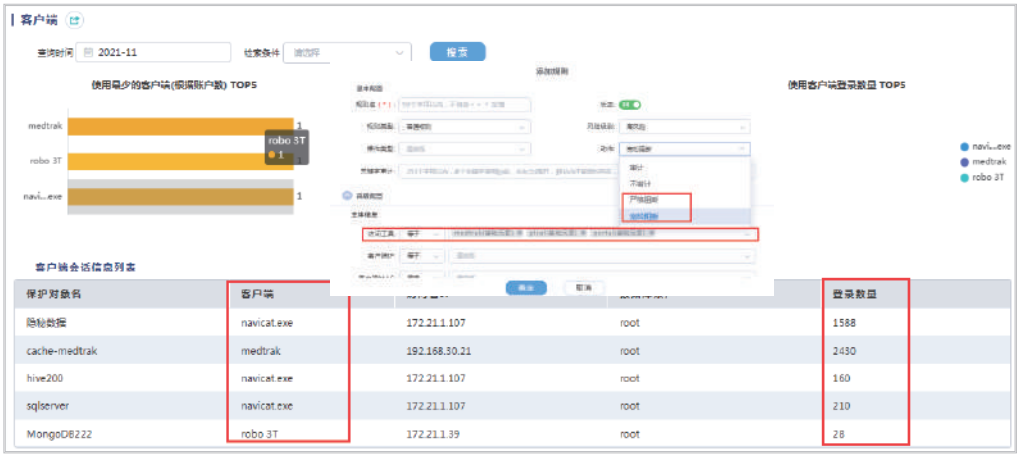
内置防攻击规则，拒绝SQL注入等黑客攻击

规则名	规则类型	规则级别	启动状态
内置 默认_新用户	普通规则	关注行为	ON
内置 默认_注入参数是字符	普通规则	低风险	ON
内置 默认_搜索时没过滤参数的	普通规则	低风险	ON
内置 默认_用户和特权管理	普通规则	关注行为	ON
内置 默认_疑似sql注入1	普通规则	低风险	ON
内置 默认_疑似sql注入2	普通规则	低风险	ON
内置 默认_测试权限结构	普通规则	低风险	ON
内置 默认_疑似sql注入3	普通规则	低风险	ON
内置 默认_对象更改	普通规则	高风险	ON
内置 默认_对象删除	普通规则	高风险	ON

支持对 SQL 注入、跨站脚本攻击等黑客攻击的识别与告警

可监控非法、未知、仿冒进程，主动防御

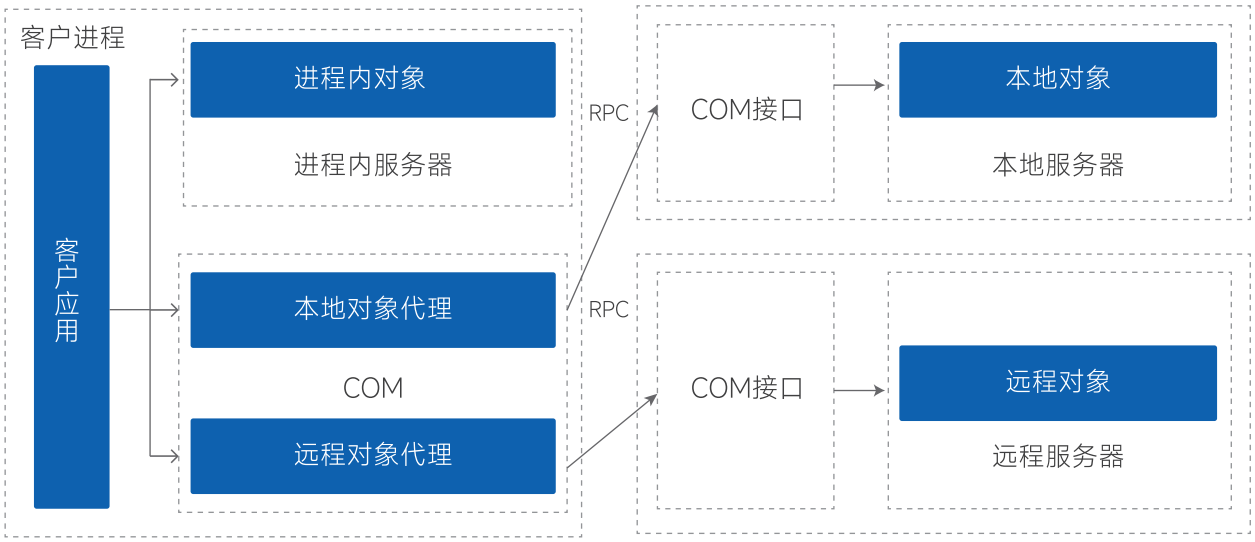
有别于一般的数据库审计产品，昂楷数据库审计系统能防范绑定变量、函数等高级别的数据查询操作，善于抓“高手”。



系统能够对进程进行监控，提前防范，真正做到事前 + 事中 + 事后全方位的防护体系

突破“三层架构”的行业难题

三层架构模式已成为当前信息系统的主流框架，但三层架构导致信息割裂，让准确定位到访问者的身份成了行业难题。昂楷数据库审计系统支持应用 http 审计、B/S及C/S方式的COM组件审计，特别是针对采取“COM/DCOM/COM+”等组件的三层架构体系，昂楷科技独创组件穿透技术，可提取工号（账号），能准确定位到人，下图以COM组件为例：




添加为系统语句
事件回放
保护对象： cache-medtrak
满足规则： select查询
风险级别： 中风险
用户
访问者： 应用测试账号
应用账号： ceshi
数据库账户： root
操作系统用户名： ankki
客户端
操作系统主机名：
地址： 192.168.30.21：1164
MAC： 6C:50:4D:AE:9D:C0
客户端进程： medtrak
数据库
数据库类型： Cache
地址： 192.168.2.3：1972
数据库名： bs_audit
操作类型：
表名： audit_record
字段名： *
操作回应： 成功
操作耗时： 0.019毫秒
操作描述： 应用测试账号用户对bs_audit数据库[audit_record]表[*]字段进行了 操作；操作发生在：2021-10-26 14:26:49，使用的电脑IP为：192.168.30.21，电脑物理地址（MAC地址）为：6C:50:4D:AE:9D:C0
操作语句： trnMEDDATA $$LData^DHCSTDISPSTATDOC(P0,P1) 407701001 418830 407701001 00:00:00 00:00:00 SSSYF-手术室药房 0 407701001 吗啡注射液(10mg) 支(10mg) 1 4.0900

支持SQL Server加密审计，支持MySQL数据库SSL加密审计

支持对加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息。

案例1：国务院国有资产监督管理委员会

客户简介

国务院国有资产监督管理委员会是中华人民共和国国务院的特设机构，根据授权，代表国家履行出资人职责，监管中央所属企业（不含金融类企业）国有资产，加强国有资产的管理工作，承担监督所监管企业国有资产保值增值的责任。

国务院国有资产监督管理委员会
State-owned Assets Supervision and Administration Commission of the State Council

需求痛点

新平台： Hadoop 大数据平台

新数据库： 非结构化 NoSQL 分布式数据库 HBase

数据量大： 数据整合共享，数据量达到 PB 级

实施效果

- 部署大数据安全审计系统
- 针对国有资产敏感信息、与国际合作的数据重点监控
- 全面监控各种访问方式，如 hue 操作、Hive 工具等
- PB 数量级下全面审计，不漏审、不误审，为国资委大数据平台的核心数据安全保驾护航

案例2：辽宁省公安厅

客户简介

辽宁省公安厅是辽宁省人民政府下设主管全省公安工作的职能部门，公安厅受省政府、公安部的双重领导。各市、县（县级市、区）设有公安局（分局），在镇、乡、街道设派出所。公安局（分局）和派出所，分别接受同级人民政府和上级公安机关领导。

辽宁省公安厅

需求痛点

目前，辽宁省公安厅已基本建立了以身份认证、授权访问、一机两用、边界防护、入侵监测、安管平台、安审平台等为主体的安全保障体系，有效地保障了公安信息系统安全。但随着辽宁省公安厅公安信息化向 “大整合、高共享、深应用”快速发展，公安信息资源种类和数据激增，信息集中度和敏感度明显增加，信息应用和共享方式日趋复杂。为了防止数据盗取、越权访问、数据篡改等现象威助到公安信息网络安全，对公安形象造成负面影响，如何保障数据库的安全、稳定和高效运行成为辽宁省公安厅下管理部门的重要工作内容。

实施效果

通过部署昂楷数据库审计系统，一方面很好地解决了辽宁省公安厅数据库的安全隐患，支撑公安机关的业务系统稳定运行，另一方面，落实与执行了国家政策法规，保障了辽宁省公安厅的对外监督与内部管理机制。整个方案实现了对数据库访问与操作行为的全面监测与审计，值得一提的是，所有的接口数据均在数据库审计系统的监控下， 对任何接口所进行的操作一目了然，并且已删除的内容可进行回溯、取证，有助于加强公安信息网络安全管理。

案例3：首都医科大学附属北京安贞医院

客户简介

北京安贞医院成立于1984年4月，北京市心肺血管疾病研究所成立于1981年9月，二者为一个医疗科研联合体，集医疗、教学、科研、预防、国际交流五位一体，是以治疗心肺血管疾病为重点的大型三级甲等综合性医院。北京安贞医院是首都医科大学第六临床医学院，1994年被 WHO&UN1CEF评为国际爱婴医院，是北京2008年奥运会定点医院，连续多年被评为首都文明单位。

需求痛点

该项目是北京安贞医院三级等保建设中关键的一环。医院采用东华软件医疗信息化系统，采用了国际医疗行业广泛使用的新一代后关系型数据库Caché，由于该数据库的架构与传统的关系型数据库架构差别巨大，长期以来，行业内没有厂商能够支持对其M语言进行审计，无法真正做到对Caché数据库的全面审计。

实施效果

昂楷数据库审计系统独家、全面支持对采用新一代后关系型数据库Caché信息化系统的监控，为医院数据库提供安全审计及防止非法统方服务，既保障了医院核心数据安全，又满足了公安部信息安全等级保护的要求。在北京卫计委医疗行风大巡查中，大批医院被责令整改，安贞医院独获表扬！

案例4：中国石化九江石油化工总厂

客户简介

九江石化作为目前全国首批智能制造试点示范企业，从2013年开始建设智能工厂，并形成了可推广的智能工厂应用框架和建设模板，成为流程型行业特别是石化行业智能化改造的样本。

需求痛点

- 工业自动化控制数据的破坏;
- 生产、营销、供应链等信息的泄露;
- 实时数据库独特的NoSQL数据结构，缺乏针对性的解决方案;
- 实时数据库所用OPC接口协议的特性，常规安全解决方案无效;
- 第三方维护人员及内部用户对数据库的访问操作行为缺乏有效监控手段。

实施效果

- 同时为工业实时数据库和传统关系型数据库提供数据安全防护，及时发现并有效遏制核心生产控制数据的破坏;
- 规范第三方维护人员及内部用户的数据库操作行为，对违规行为及时发现实时预警，并能实现过程回放与电子取证;
- 满足企业信息化内控、信息安全等级保护等合规性要求。

案例5：上海电信政务云

客户简介

中国电信上海公司拥有中国电信集团内最大的城市电信网络，为超过2200万用户提供包括移动通信、宽带互联网接入、信息化应用及固定电话等产品在内的综合信息解决方案，始终保持上海地区通信市场的领先地位。

需求痛点

- 众多部委办局业务持续接入，应用类型繁多，交互频繁，无法保证数据安全；
- 无法保证租户接入云端后依旧能满足等级保护安全相关规定；
- 对于业务访问数据库操作无法进行审计，并且审计的粒度严重不够，查询、追溯困难；
- 云环境下，租户无法全面了解当前业务访问数据库的情况，无法全面监测当前数据库安全情况。

实施效果

- 满足租户对于等保合规需求；
- 租户只需要通过大屏就能实时的、详细的展现出了当前数据库安全状态，一目了然；
- 实现了云环境下对租户数据库的独立审计，不需要依赖数据库自身审计日志；
- 大大提高了数据库审计的粒度，满足了租户对数据库审计快速查询、追溯方便的需求。

案例6：昆仑银行

客户简介

昆仑银行股份有限公司原名克拉玛依市商业银行股份有限公司，前身系克拉玛依市城市信用社，2010年4月，更名为昆仑银行，寓意磅礴发展的“昆仑”商号为银行注入了强大的品牌价值。

需求痛点

银行业，是金融行业个人隐私泄露的 “重灾区”，客户私人信息被泄露、被遗弃的传闻不绝于耳。通信、计算机技术等高科技手段在银行业广泛运用，网络银行迅速发展，给人们带来方便的同时，利用信息网络技术的犯罪也在迅速增长。面对“泄密门”，恐慌是没有用的，用户修改密码只是“治标”，如何建立健全信息安全制度保障、营造互联网健康环境才是“治本之策”。

实施效果

通过部署3台昂楷数据库审计系统，根据多年数据库安全经验提供报表支持，实现数据库异常操作监测报警，并提供多种告警方式通知相关人员处置，采用独立审计的工作模式，不对现有系统造成任何影响，弥补了因数据库系统内置日志审计而带来的缺陷。

部分典型客户名录

注：昂楷数据库多重审计系统已广泛应用于政府教育、医疗卫生、金融证券、电信通信、商业企业等诸多行业，得到客户的普遍认可及好评。

公检法司		
湖南省公安厅	安徽省公安厅	辽宁省公安厅
南京市六合区公安局	连云港市公安局	青海省森林公安局
茶陵公安局	东莞市第三人民法院	安徽省巢湖监狱

政府		
某省国家安全厅	中国网安	国务院国资委
深圳智慧城市	武威市雪亮工程	北京经济开发区财政局
内蒙古自治区财政厅	上海市财政局	吉林市人力资源和社会保障局
郑州市人力资源和社会保障局	昆明市人力资源和社会保障局	东莞市人力资源局
山西省公路局	甘肃省税务局	陇南市住房公积金管理中心
宝鸡市审计局	包头市规划局	三明市住房和城乡建设局
深圳坪山新区社会建设局	抚顺市房屋管理交易中心	清远市公共资源交易中心
南昌国土资源局新建分局	云南省委统战部	昆明市保密局

云安全		
UCloud	青云 QingCloud	腾讯云
华为云	金山云	有孚云

医疗

北京协和医院	天津市卫健委	深圳市南山区卫生局
东莞市卫生局	濮阳市卫生局	连州市卫生局
首都医科大学附属北京安贞医院	首都医科大学附属北京安定医院	首都医科大学附属北京友谊医院
首都医科大学附属复兴医院	北京中医药大学东直门医院	中国医科大学航空总医院
首都医科大学宣武医院	秦皇岛第一医院	沈阳市第九人民医院
中国人民解放军第四一一医院	中国人民解放军第一八八医院	中国人民解放军第一六九医院
中国人民解放军第八十九医院	郑州大学第一附属医院	河南省人民医院
济宁医学院附属医院	重庆医科大学附属口腔医院	成都医学院第一附属医院
成都大学附属医院	湖北省中医医院	西安交通大学第二附属医院
西安医学院第一附属医院	甘肃省中医院	华北石油总医院
南方医科大学南方医院	中山大学附属第三医院	广西医科大学第一附属医院

更多客户名录

中国电信上海分公司	中国联通重庆分公司	中国移动通信有限公司研究院
500万彩票网	太平鸟集团有限公司	上海地铁
天津公交融通公用卡科技有限公司	宁夏电投西夏热电有限公司	九江石化
浙江新安化工集团	昆仑银行	鄂尔多斯银行股份有限公司
成都农商银行	江苏省农村信用社	慈溪农商银行
长安大学	西安建筑科技大学	哈尔滨商业大学
黑龙江八一农星大学	东北电力大学	湖南人文科技学院
重庆教育数据中心	郴州广播电视大学	东莞理工学院

注：排名不分前后

引领数据安全潮流
护航业务核心安全

深圳昂楷科技有限公司

地址：深圳市前海深港合作区南山街道桂湾五路123号前海大厦T2栋6楼
电话：400-622-8990
网址：www.ankki.com
E-mail：support@ankki.com

版本号：Ankki-AAS-20220507-V3.0

官方微信