知道创宇
KNOWNSEC.COM

创宇智图数据库审计与防护系统

产品白皮书

2021-05-12

北京知道创宇信息技术股份有限公司

更好更安全的互联网

文档控制

文档名称	创宇智图数据库审计与防护系统产品白皮书
保密级别	内部公开
拟制	
审核	
标准化	

版本控制

版本	提交日期	相关组织和人员	版本描述
V1.0	2021-05-12	辛宇	创建

目 录

1 概述

1.1 背景介绍

随着政府部门、金融机构、企事业单位、商业组织等对重要数据库业务系统和数据库应用系统依赖程度的日益增强，数据库安全及数据安全的问题受到普遍关注。由于信息化建设、业务增长、系统上云等因素，在各系统中的数据库服务器也不断增加，对数据库的管理的方式和通道也日趋复杂多样。在如此繁杂的情况下，引发了如滥用特权账号、滥用合法权限、身份验证不规范、备份数据暴露、审计记录不足等各类安全问题，并加大了 IT 内控审计的难度。

与此同时，数据安全问题日益突出，如系统和数据库的通信协议存在漏洞、SQL 注入攻击、拒绝服务攻击、权限和账号被盗、弱口令等，给攻击者留下了可趁之机，也给管理者带来了管理层面的麻烦与困难。

根据威瑞森电信公司（Verizon）发布的《2017 年的数据泄露调查报告》统计：

- 在风险比例方面：25%是内部威胁、75%是外部攻击；在外部攻击中，51% 的网络攻击涉及到有组织有预谋的犯罪集团，18%的外部攻击涉及国家背景。
- 在勒索软件方面：与 2016 年的报告数据相比，勒索攻击次数上升了 50%；而且勒索软件变得越来越高级，对数据的攻击具备潜伏性、破坏性和瞄准性。
- 在数据泄露原因方面：62%的数据泄露与黑客攻击有关、81%的的数据泄露涉及到撞库或弱口令；也就是说，人们使用密码的习惯依然不太好，绝大部分人并没有养成定期修改密码的习惯。
- 在行业分布方面：金融行业依然首当其冲，24%的数据泄露事件和金融机构有关，其次是医疗保健行业 15%，再往后是销售行业 15%以及公共部门 12%；其中医疗行业是勒索的重灾区，真可谓“不给钱就撕票”。
- 在报告中，Verizon 还建议企业可利用威胁实时智能分析技术，以缩短威胁响应时间。

1.2 风险分析

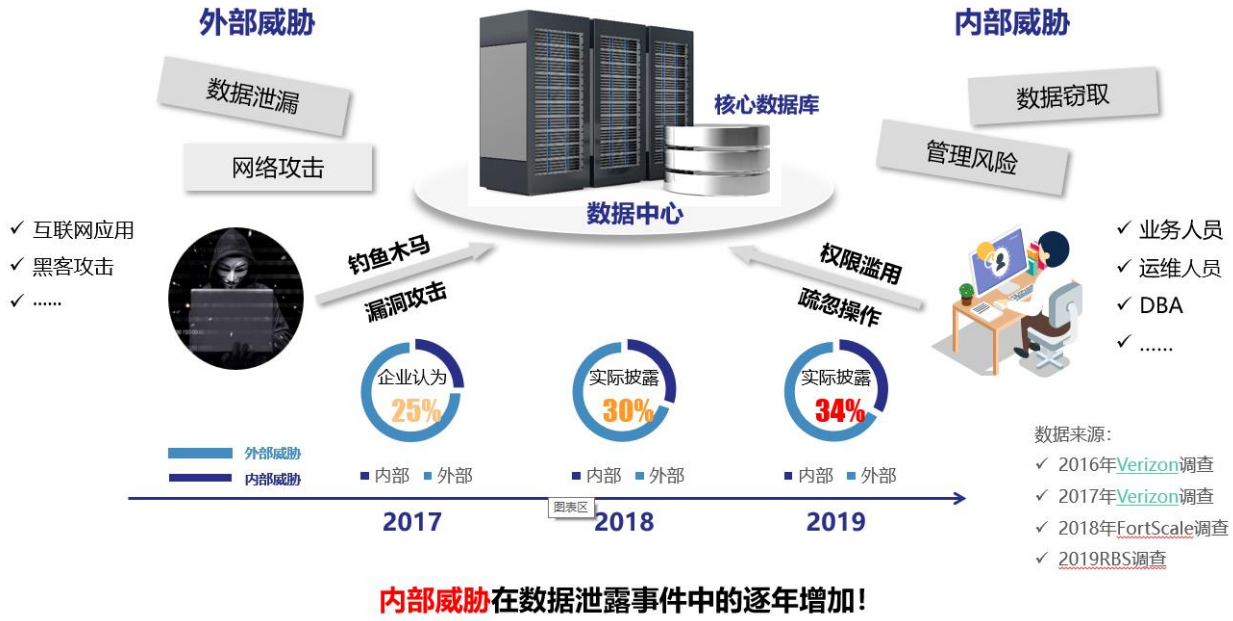
数据库安全风险及需求，可以归纳为以下几个方面：

1.2.1内部访问风险

有 25%的数据库威胁是来自内部，如 DBA、数据库开发人员、操作人员等；容易出现权限滥用、误操作、弱口令等问题，给管理带来了很大困难，更加无法进行有效的记录和预警。

1.2.2外部访问风险

有 75%的数据库威胁是来自外部，互联网访问者、外包人员通过互联网途径访问；容易出现越权操作、恶意访问、账号密码泄露等问题。甚至容易被黑客攻击，如 SQL 注入、零日攻击等，同样给管理带来了很大的难度。



内部威胁在数据泄露事件中的逐年增加!

1.2.3传统安全防护手段的缺陷

面对外部访问威胁，通常的做法是利用传统的安全系统进行防护，如防火墙、IPS、IDS 等，但是面对诸如 SQL 注入、零日攻击等威胁，常常束手无策。

面对内部访问威胁，传统安全系统也无法有效控制或记录数据库产生的风险。

1.2.4系统自身审计的缺陷

应用系统或数据库系统，自身都带有系统日志，具备一定的分析作用。

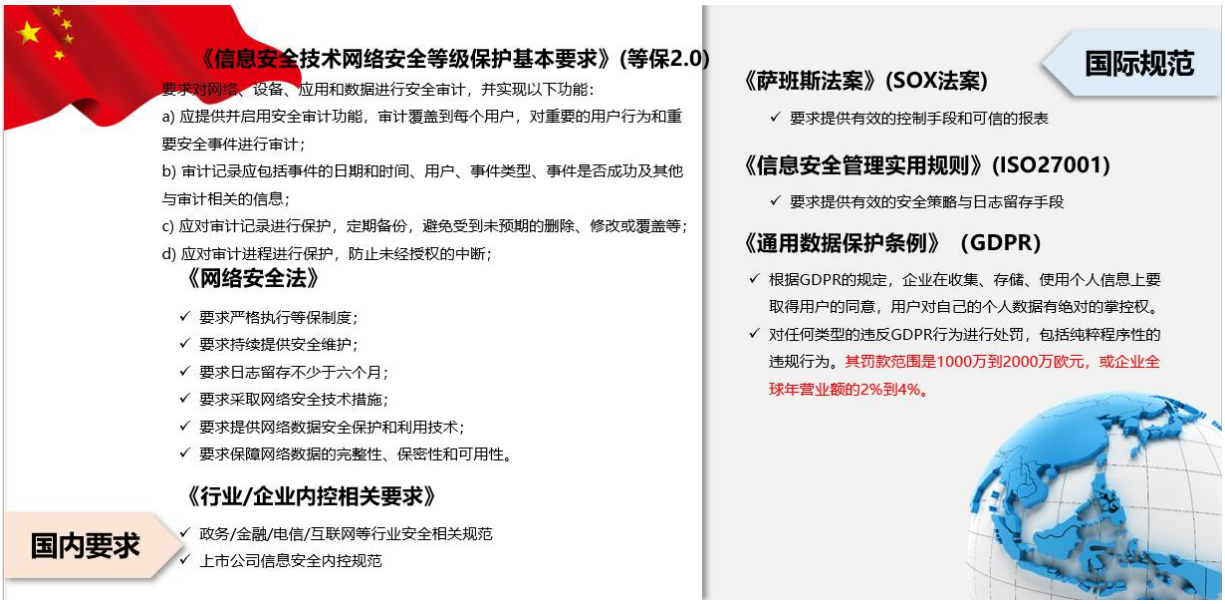
但是，系统自身的日志不仅可读性差，而且容易被篡改，更加不具备第三方独立性和权威性；甚至，开启自身记录功能之后，直接影响了系统的性能以及稳定性。

1.2.5合规要求

随着大数据时代的到来，数据已经深入并融合到社会的各个阶层和组织中，数据的安全已经成为社会安全的重要组成部分。如何应对海量数据应用带来的各种威胁，已经成为上至国家、下至组织和个人关注的重点问题之一。

目前国内、国际的很多标准、法案法规都要求相关组织单位建设安全的审计系统，并确保审计信息是安全、完整、可查及唯一的：

- 信息安全等保要求访问来源识别、数据审计、日志记录、审计报表等。
- ISO27001 标准要求记录用户访问、意外和信息安全事件的日志，以便为安全事件调查取证等。
- SOX 法案要求组织设计和执行了适当的数据保护技术，以确保财务报表数据的可靠、可信等。
- 企业内控规范要求企业严格执行规范要求，以加强和规范内部控制、提高风险防范能力等。
- 等保 2.0 更是加强了对数据及数据库安全的要求。

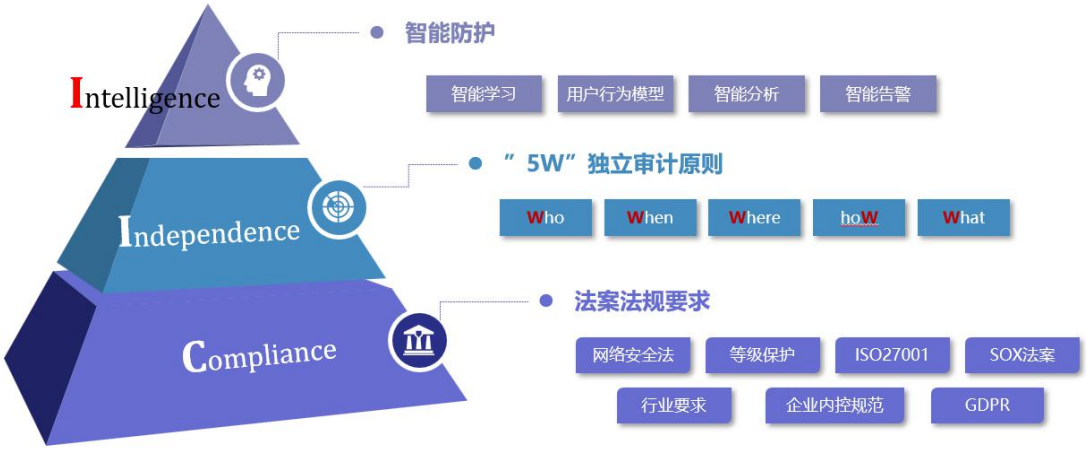


2 产品介绍

创宇智图数据库审计与防护系统是信息基于多年数据库安全的理论和实践经验积累的基础上，结合各类法令法规（如网络安全法、SOX 法案、等级保护、PCI、企业内控管理等）对数据库审计的要求，自主研发完成的业界首创智能自动学习、自动建模、风险自识别、细粒度审计、精准化行为告警、全方位的数据库安全审计产品。

创宇智图数据库审计与防护系统基于“CII”设计理念，设计出针对数据库安全的专业解决方案，为客户的核心数据库资产构建“最后一道安全防线”。

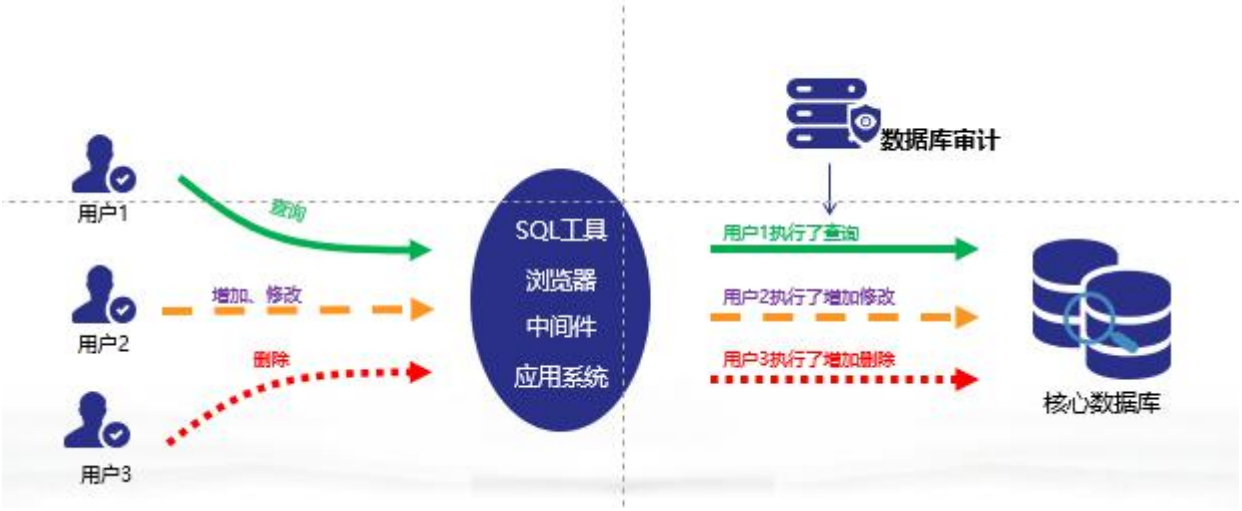
“CII”设计理念：为数据库构建“最后一道安全防线”！



可以帮助您解决以下问题：

- 识别越权使用、权限滥用，管理数据库帐号权限
- 自动跟踪敏感数据访问行为，及时发现敏感数据泄漏
- 自动检测数据库系统运行弱点、发现 SQL 注入等漏洞
- 自动创建数据库业务模型、及时发现异常 SQL
- 实时监测 SQL 交互量、TCP 会话、风险行为等态势
- 为数据库管理与优化提供决策依据
- 满足法律、法规要求，提供符合性报告
- 低成本且有效推行 IT 管理制度

创宇智图数据库审计与防护系统支持旁路审计、代理审计和插件审计三种工作模式，来获取数据流量，通过对数据流量进行深度解析来实现对数据库的审计，帮助用户实时统计访问数据库的请求和风险，提升数据库运行监控的透明度，降低人工审计成本，真正实现数据库全业务运行可视化、日常操作可监控、危险操作可控制、所有行为可审计、安全事件可追溯。

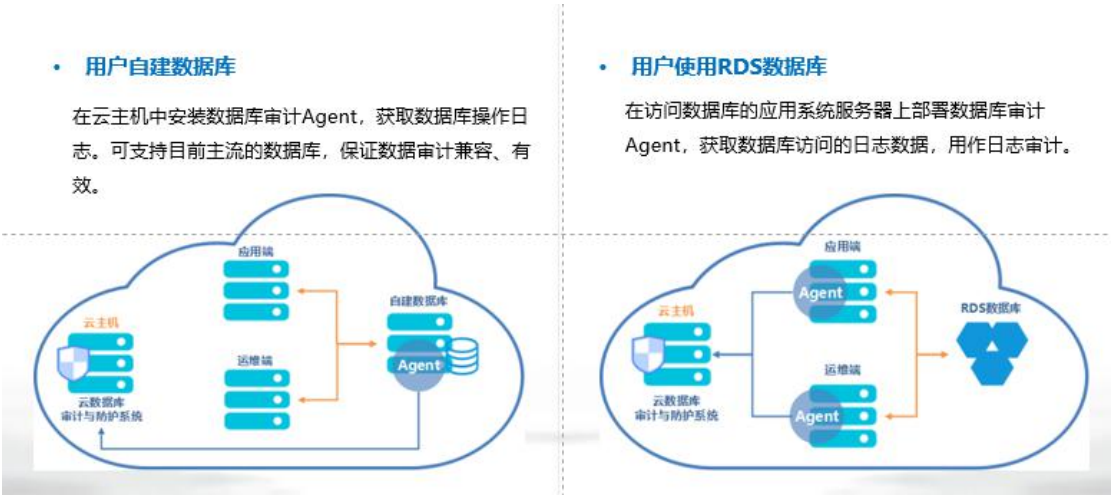


创宇智图数据库审计与防护系统提供灵活的告警策略、细粒度的审计日志和合规性的报表，解决客户的核心数据库面临的“越权使用、权限滥用、权限盗用”等安全威胁，满足各类法令法规对数据库审计的要求，广泛适用于“政府、金融、运营商、公安、能源、税务、工商、社保、交通、卫生、教育、电子商务及企业”等所有使用数据库的行业。

3 产品优势

3.1 云环境的部署与审计

创宇智图数据库审计与防护系统不仅适用于物理环境，而且可直接部署在云端，帮助客户防护和审计云端数据库；可以适用于公有云、混合云的环境



3.2 全面的数据库类型

不仅支持主流的数据库，如 Oracle、SQLServer、MYSQL、DB2、Informix、Sybase；而且支持国产数据库达梦、人大金仓、GaussDB、南大通用、神州通用和专业的数据库 PostgreSQL、Greenplum、Cache，同时还支持云数据库及大数据组件 Hbase、Hive、Hdfs、Elasticsearch、MongoDB 的解析与审计。

主流数据库 Microsoft SQL Server SYBASE MySQL ORACLE IBM DB2 Informix SOFTWARE

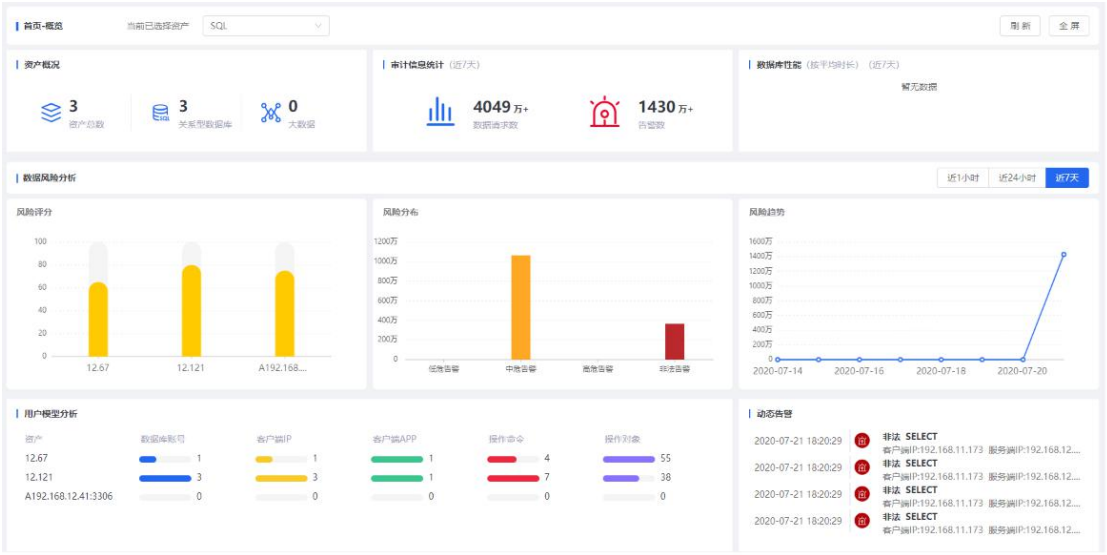
国产数据库 达梦数据库 人大金仓 Kingbase GBASE 神舟通用

专用数据库 PostgreSQL Greenplum Cache

大数据 APACHE HBASE Apache Hive mongoDB elasticsearch

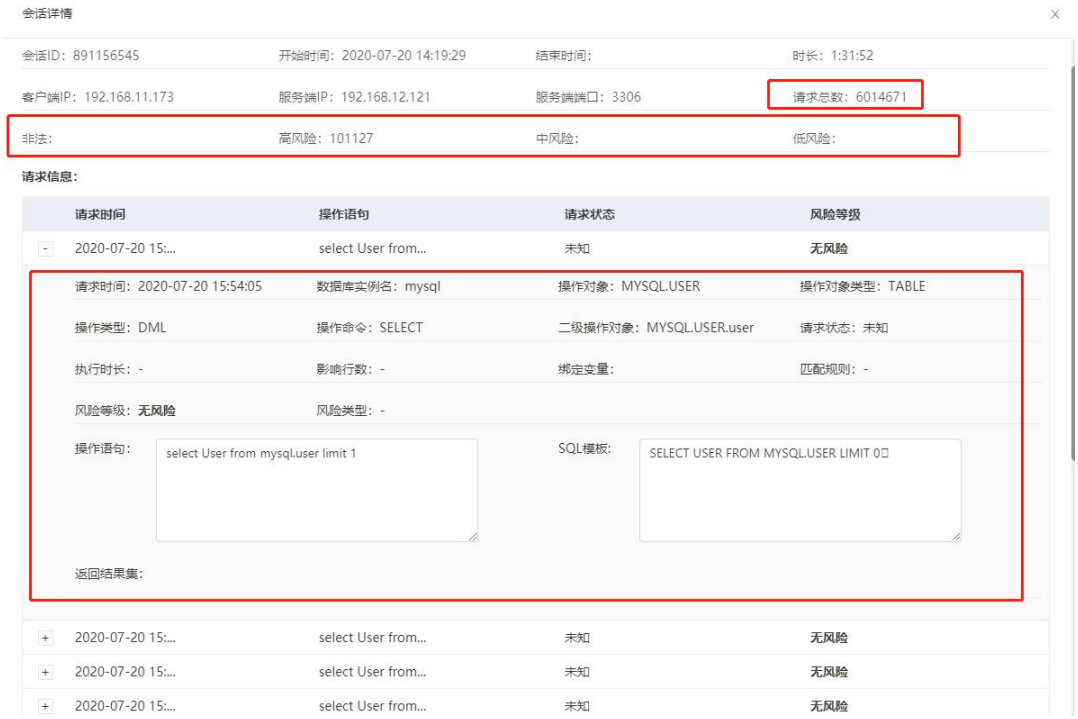
3.3 实时风险趋势

创宇智图数据库审计与防护系统首页通过实时分析引擎可以实时展示数据库风险分布、风险趋势、风险评分，用户行为分析、动态告警，方便管理员实时查看数据库风险趋势。



3.4 行业领先的实时会话展现

不仅可以实时展现实时在线的会话，还可以实时统计和展现会话中的请求数和告警数，让数据库的访问和数据库的风险“一目了然”。



3.5 细粒度的 SQL 审计日志

通过 5“W”的设计理念和数据流量的深度协议解析，最终实现能审计详细的 SQL 日志信息，包括，来源信息、目标信息、操作内容、字段信息、语句类型等二十多种数据库请求日志信息。

支持对访问数据库的源主机名、源主机用户、源应用程序等信息的审计，以满足追踪溯源的要求；

支持 SQL 操作响应时间、select 操作影响行数、返回结果集，数据库请求状态的审计；

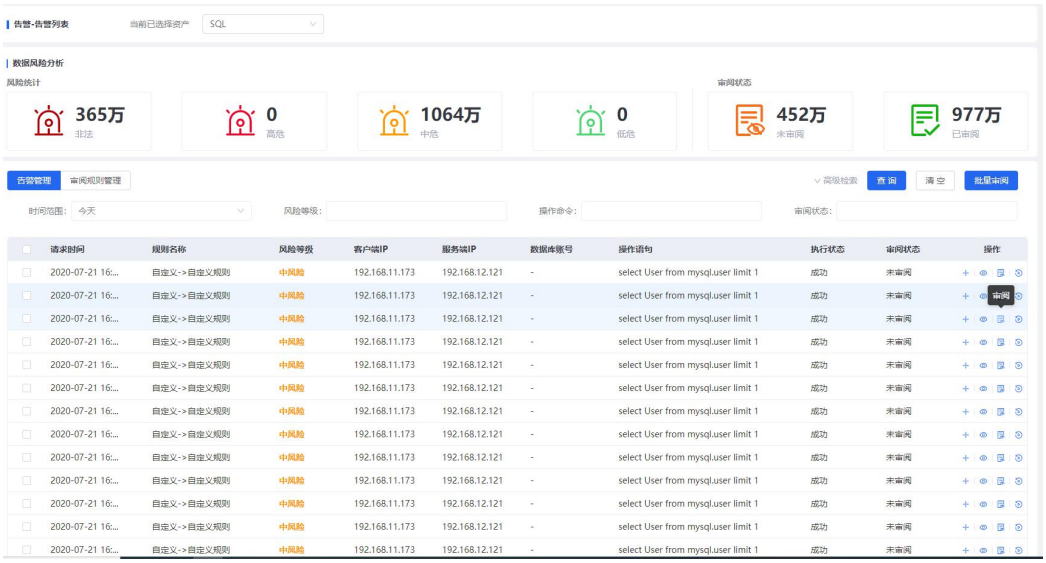
支持数据库操作类、表、视图、索引、触发器、存储过程、域、schema、游标、事物

等各种操作对象的 SQL 语句的审计；

支持 DDL、DML、DCL 等各种对数据库操作类型的审计。

3.6 数据风险分析及告警审阅

创宇智图数据库审计与防护系统通过提供了专用的告警管理功能，详细记录每一告警日志，并且可以对告警信息进行审阅，填写审阅意见。

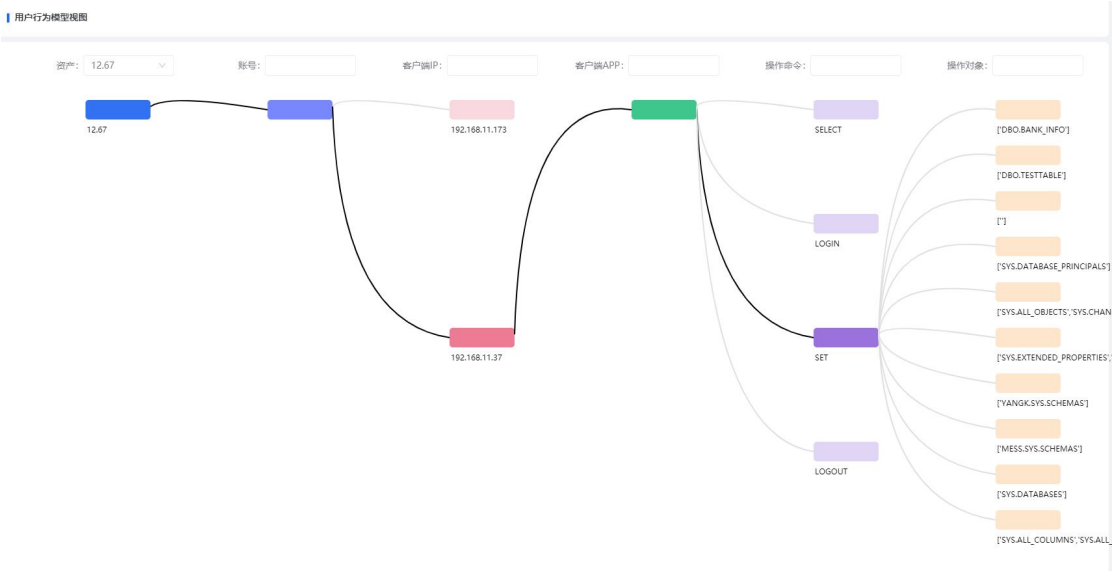


3.7 智能学习，自动建模、异常告警

创宇智图数据库审计与防护系统利用 secsmart 审计引擎，根据账号、SQL 语句特征和访问特征等内置了智能的自动建模机制，最终实现正常与异常的数据分析能力；不仅帮助客户梳理常态化的数据类型，而且可以有效快速的发现异常访问；一旦发现异常则及时告警并通知管理员。

3.8 用户行为分析

创宇智图数据库审计与防护系统基于深度分析技术引擎。将资产、用户账号、客户端 IP、客户端工具、操作命令、操作对象使用曲线连进行关联，通过层层钻取的方式生成用户访问轨迹，清晰的展示用户通过哪个 IP、什么客户端工具，对数据做了哪些操作，且支持用户自定义下钻分析。



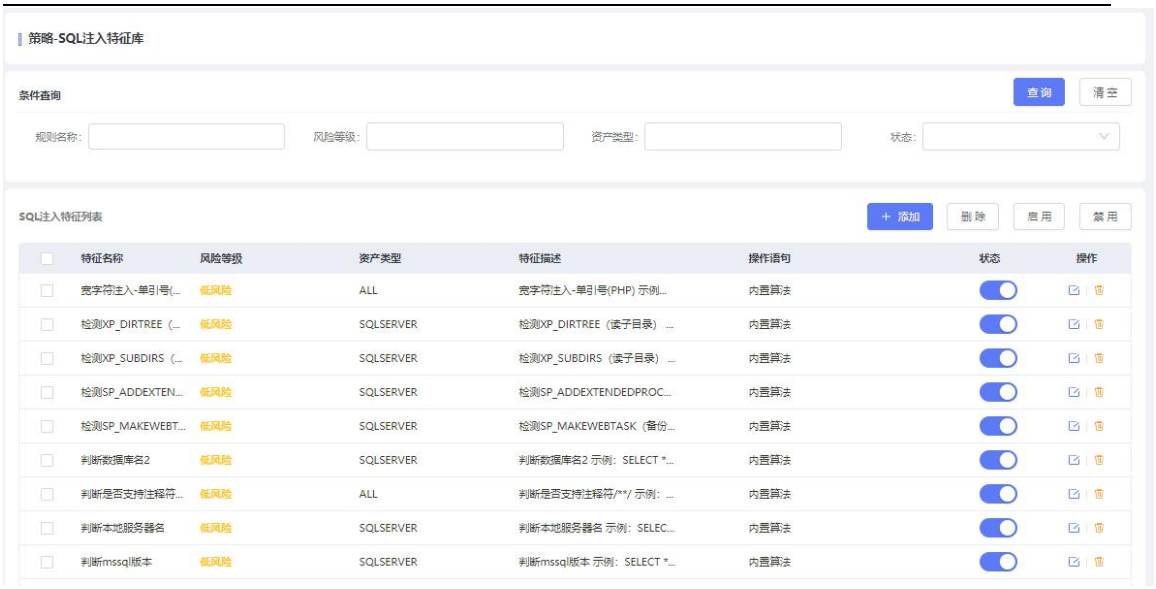
3.9 会话回放

创宇智图数据库审计与防护系统，支持在检索、告警、会话中选择任意语句进行 SQL 语句回放，完整还原用户的访问行为，也可以选择从当前开始播放，播放过程可随时暂停、

继续，且可以在播放过程中选择任意语句，播放前后 XX 条，减少用户筛选过程。

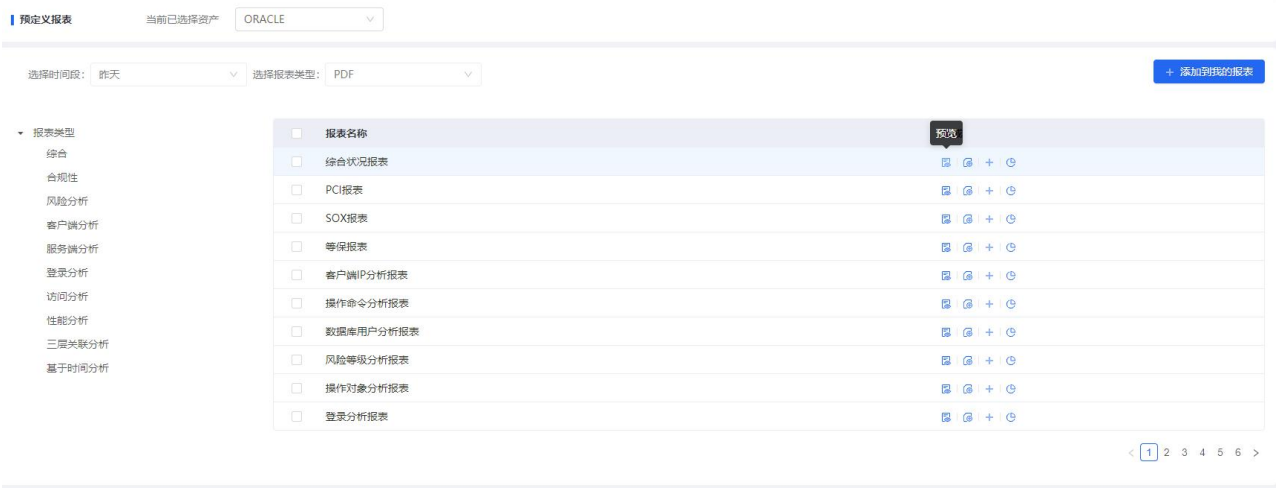
3.10 威胁自识别，自告警机制

创宇智图数据库审计与防护系统中内置了丰富多样的威胁特征库和风险规则库，可以有效的对 SQL 注入、缓冲区溢出、暴力破解数据库等行为进行及时告警，为管理层提供风险分析依据。



3.11 内置丰富的合规性报表

创宇智图数据库审计与防护系内置了通用及丰富的报表模板，支持报表预览、定时发送、报表收藏等实用功能；同时，也按类型对报表进行分类：包括综合报表、合规性、风险分析、客户端分析、服务端分析、登陆分析、访问分析、性能分析、等 10 种报表类型，方便用户对报表进行查找和使用。

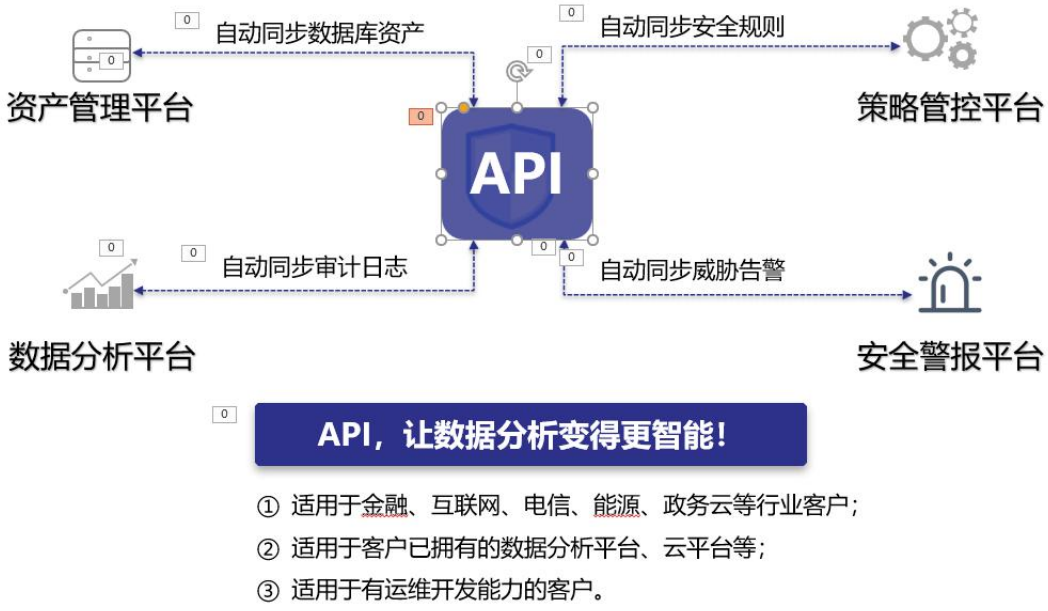


3.12 最开放的、最全面的接口联动

系统开放了全部数据接口，如审计数据接口、告警数据接口、配置接口、策略接口等，方便用户对接第三方设备，进行日志管理，策略下发，让数据分析变得更加智能，让用户使用更加方便。

首页模块	资产列表	趋势图	风险统计	最新告警	
审计模块	告警	检索	会话		
分析模块	统计分析	资产列表	用户操作		
策略模块	黑白名单	自定义	智能防护	网络防护	漏洞攻击
报表模块	报表模板	定时报表	报表生成	报表下载	
系统模块	设备状态	设备配置	登陆设置	数据维护	
登陆模块	登陆接口	登出接口	修改密码接口		

允许第三方平台对接并调用创宇智图数据库审计与防护系统的接口；让数据分析变得更智能。

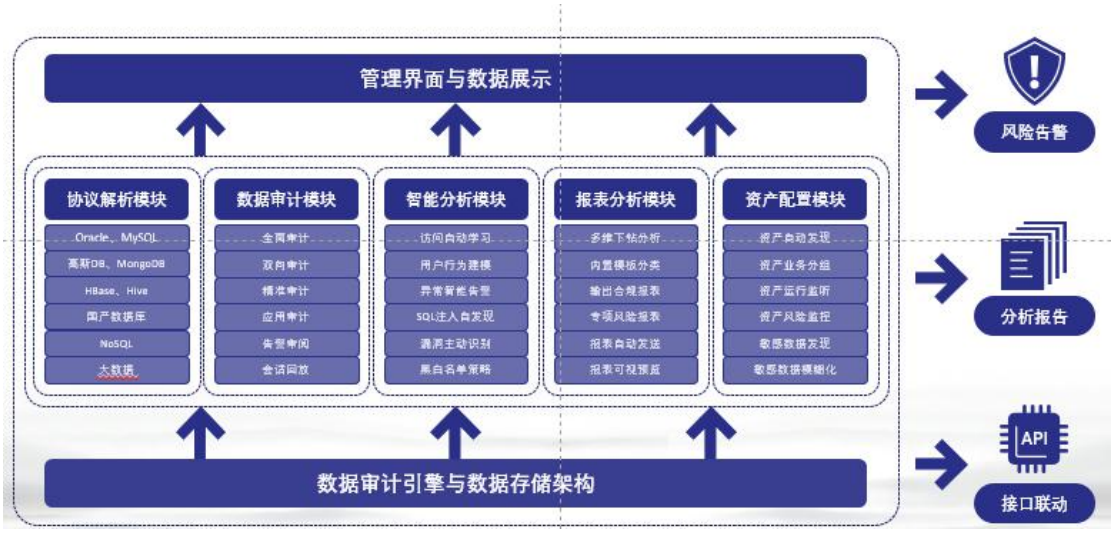


API，让数据分析变得更智能！

① 适用于金融、互联网、电信、能源、政务云等行业客户；
② 适用于客户已拥有的数据分析平台、云平台等；
③ 适用于有运维开发能力的客户。

4 产品功能

创宇智图数据库审计与防护系统不仅提供了有价值的功能，而且提供了全面的产品功能，更有利的帮助客户实现数据安全解决方案。



4.1 资产发现

基于深度协议分析技术，对网络中的流量进行分析，实现对网络中的数据库资产进行自动识别，并归类分组添加到审计系统，整个过程无需人工添加，实现数据库审计。

4.2 精确审计

通过对 SQL 语句进行深度协议解析，可审计到语句的执行结果（成功或失败）、执行时长、返回行数、绑定变量值、返回结果等内容，帮助客户有效的提升审计内容的精确性。

4.3 安全策略

系统内置审计策略和漏洞特征库，用户只需一键开启便可使用，还提供了黑白名单、自定义告警规则，方便用户自定义配置策略，帮助用户及时发现威胁，并进行告警。

4.4 实时监控

能对数据库的在线连接的会话进行实时监控，帮助客户更好的了解数据库并发会话、SQL 请求数、告警数、等多种数据访问的状态。

4.5 风险告警

提供了邮件、短信、ftp、syslog、snmp 等告警方式，可以自主选择告警方式。

4.6 告警审阅

创宇智图数据库审计与防护系统提供告警审阅功能，可对告警日志进行审阅，并填写审阅意见，可对告警进行批量审阅和自动审阅。

4.7 IP 翻译

创宇智图数据库审计与防护系统提供 IP 翻译功能，可对客户端 IP、服务端 IP 进行翻译，修改后可支持在报表中显示为业务名称，方便用户查看告警日志和审阅报表。

4.8 多维分析

创宇智图数据库审计与防护系统支持对审计日志进行分析，可以按照客户端 IP、数据库账号、操作命令、风险等级、风险类型等 20 多个维度进行分析，且支持对审计日志进行下钻分析，帮助用户进行数据挖掘，分析完成后还可以生成报表和报表模板，进行多次使用。

4.9 系统管理

创宇智图数据库审计与防护系统提供了系统升级维护、系统运行状态监测、网络接口配置、数据存储空间大小设置等管理功能。

4.10 三权分立

创宇智图数据库审计与防护系统提供了 3 个管理员（系统管理员、安全管理员、审计管理员），分管创宇智图数据库审计与防护系统的不同功能模块，满足三权分立要求。

5 应用价值

5.1 应用改造零代价，不影响网络拓扑

创宇智图数据库审计与防护系统采用旁路部署，对现有的网络环境、业务系统、应用系统基本透明，无需改造，原有的数据库核心特性均可继续使用。

5.2 数据交互全审计，不放过任何疑点

创宇智图数据库审计与防护系统对数据库的所有交互行为进行审计，不论正常与否都进行全记录和全保存；帮助用户保存至少 6 个月的审计日志，也可以将审计数据导出备份存储。一旦发生安全事件，可快速定位追溯。

同时，还支持 DDL（Create、Drop、Alter）、DML（Insert、Delete、Update）、DCL（Grant、Vevoke）、TCL、RCL、Login、Logout 等各种对数据库的操作类型的审计

5.3 实时会话展现，让数据库访问“一目了然”

创宇智图数据库审计与防护可以实时展现在线的会话列表，帮助用户实时了解数据库的访问情况：来源 IP、访问时间、登录账户、目标数据库、SQL 语句、执行结果、访问时长等等。

5.4 实时数据监测，让数据库风险“不再隐蔽”

通过创宇智图数据库审计与防护系统不仅可以实时监测数据库会话中的风险级别，而且可以监测到每个会话中含有的风险数量。通过快速的智能检索功能，可以帮助用户及时定位风险 SQL 语句。

5.5 风险智能分析，数据威胁自动预警

创宇智图数据库审计与防护系统内置了丰富多样的特征库，如漏洞特征库、SQL 注入特征库、威胁访问特征库等等。对数据威胁访问提供自动的、及时的预警。一旦发生数据威

胁，自动通知管理员。

创宇智图数据库审计与防护系统能对数据库的运行状态进行分值评估，帮助用户及时了解数据库的风险状况，为管理层提供了数据安全改进的依据。

在创宇智图数据库审计与防护系统中有数据库自动学习建模功能，通过一段时间的学习，可以建立敏感数据的访问特征模型，一旦有新的行为发生时就会比对其是否符合特征模型，同时根据新行为与特征模型匹配程度形成高、中、低三个不同级别的预警。在预警信息中包含了是什么人操作、怎么操作、操作了什么、在什么时候、什么地方操作等内容。

5.6 输出合规报表，满足法案法规

创宇智图数据库审计与防护系统可定期的出具审计报表，以统计当月的违规统方情况。在创宇智图数据库审计与防护系统中有内置 50 多种报表，可以按照告警规则名称、违规账户、违规 IP 等形成丰富的报表。让用户能够及时的了解整体数据库的情况。

同时也有一些审计信息统计类报表能够帮助信息科数据库管理员了解数据库的运行情况，包括整个数据库到底包括了哪些帐号、每个账户一般都会在哪些地方、哪些时间，通过哪些工具去做一些什么样的操作。也能够统计数据库的流量、操作熟练、操作类型等。