Sinoregal dbAudit

星瑞格数据库安全审计系统

产品白皮书

福建星瑞格软件有限公司

目录

一、产品背景

文件从纸张到数字化的过程，重要文件与敏感数据不再存放在传统保险箱中，取而代之是以数字形态存在于企业数据库中。过去二十多年来，企业采用了防火墙、防病毒软件、入侵检测与漏洞扫描等工具阻挡针对企业信息系统特别是数据库的攻击，防止企业敏感数据外泄。随着企业信息化的快速发展，企业信息孤岛逐渐被打破，信息互联互通，企业数据库信息的价值越来越高，敏感数据在企业内部随处可见；随着互联网、移动互联网的急速发展，企业数据库信息的可访问性得到了极大提升，数据传播方便快捷；数据库信息资产安全面临着空前的挑战。

1.1 企业信息资产安全面临严重威胁

1．外部威胁：不仅威胁的总数在增加，威胁态势也变得更加多样化，攻击者也在不断开发新的攻击途径并尽力在攻击过程中掩盖踪迹。

America's JobLink(AJL)系统被黑：2017 年 3 月，一名黑客利用美国 Job Link 系统中的漏洞劫持了 480 万个帐户，导致 480 万名求职者的个人信息被泄露。

2．内部员工的不规范操作：主要表现为：人员的职责、流程有待完善；内部员工的日常操作有待规范；第三方维护人员的操作监控失效；离职员工的后门，致使安全事件发生时，无法追溯并定位真实的操作者。

Verizon Communications(威尔逊电信)数据泄露：2017 年 6 月份，美电信巨头 Verizon 的 600 万用户数据被泄露，但直到 7 月 Verizon 才证实这一消息，并在一份声明中称数据泄漏是由该公司供应商的一名员工造成。因操作失误导致外部可进入云存储区域访问信息，而这些数据是在没有保护的亚马逊 S3 存储服务器上泄漏的，这使得任何有公共链接到云的人都可以使用这些数据。

上述事件可知：由于外部通过 web 应用系统进行的数据窃取等行为，以及合法授权者的非法或可疑访问活动，导致企业重要数据泄露而产生重大损失的事件已屡见不鲜。数据库行为审计系统作为判断用户行为合法性的重要工具，成为保护企业核心数据安全的重要一环。

1.2 现有数据库审计产品面临的挑战

1.2.1 技术挑战

1．数据库管理风险：Oracle，SQL Server 是一个庞大而复杂的系统，安全漏洞如溢出，注入层出不穷，每一次的 CPU（Critical Patch Update）都疲于奔命。一般客户出于稳定性考虑，对补丁的跟进非常延后，何况通过应用层的注入攻击使数据库处于无辜受害的状态。

2．现有的依赖于数据库日志文件的审计方法，存在诸多的弊端。比如：数据库审计功能的开启会影响数据库本身的性能、数据库日志文件本身存在被篡改的风险，难于体现审计信息的有效性和公正性。

3．大数据时代下，数据库安全审计与防护有了新的机遇和挑战：部分关系型数据库逐步被非关系型数据库取代，处理的数据量比以往

高出一个甚至几个数量级。面对新形势，数据库安全审计与防护产品需要解决对非关系型数据库的兼容问题，并具有海量数据背景下的处理能力，这是在产品转型升级过程中厂商需要直面的问题。

4．基于审计的数据挖掘也将成为未来的关注热点：通过审计，收集大量用户数据，运用大数据平台进行数据多维度关联分析，最终把有价值的客户信息呈现出来，这正是大数据时代用户所期望的。

1.2.2 政策挑战

国家政策和法规的日益完善，对数据库安全产品的要求和挑战也越来越高。近年来，随着信息技术的发展和网络安全形势的变化，等保 1.0 要求已无法有效应对新的安全风险和新技术应用所带来的新威胁，等保 2.0 适时而出，从法律法规、标准要求、安全体系、实施环节等方面都有了变化。

什么是等保 2.0？等保 2.0 全称网络安全等级保护 2.0 制度，是我国网络安全领域的基本国策、基本制度。等级保护标准在 1.0 时代标准的基础上，注重主动防御，从被动防御到事前、事中、事后全流程的安全可信、动态感知和全面审计。等保 2.0 中主要在安全区域边界、安全计算环境和安全管理中心的要求中提到审计要求。

相比于之前等保 1.0 的版本，等级保护 2.0 随着信息技术的发展经过不断的完善、更新、充实。对企业和安全审计厂商来说，有几点需要注意：

1．从条例法规提升到法律层面。等保 1.0 的最高国家政策是国

务院 147 号令，而等保 2.0 标准的最高国家政策是网络安全法。因此不开展等级保护等于违法。如果用户单位不做等级保护测评，用户单位及主管人员均需受到相关处罚及罚款。

2．测评要求更加严格：以前 4 级系统半年要测评一次，现在 3 级及以上系统每年做一次。1.0 里 60 分以上算及格，现在 75 分算及格。基本分高了，要求变得更高，过等保的难度增加。

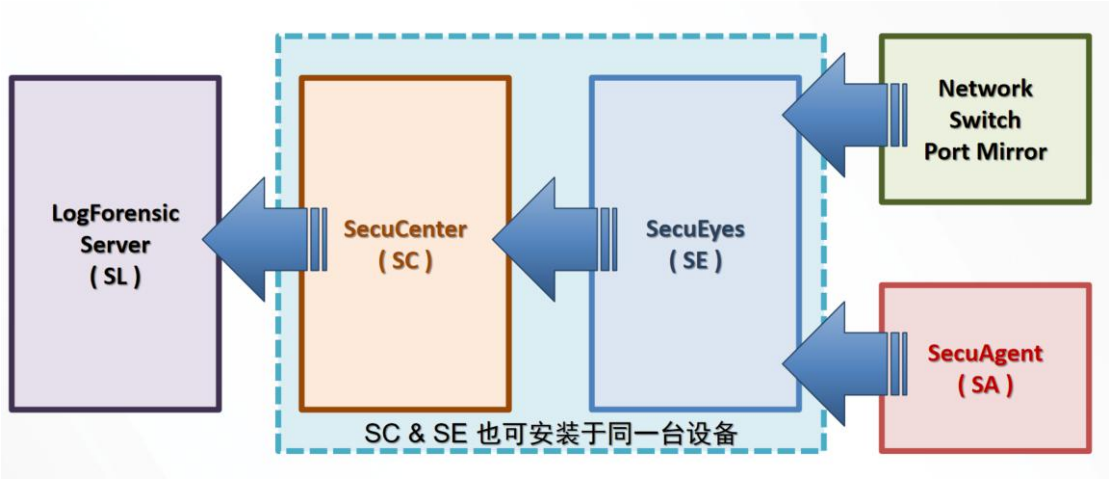
3．对象范围增加：等保 1.0 定级的对象是信息系统，等保 2.0 的定级对象扩展至基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等多个系统平台，覆盖面更广。

4．对于等保 2.0 中可信计算及密码技术的应用提出了明确要求，这将很大促进可信计算及密码技术的推广及应用。

5．等保 2.0 新增对新型网络攻击行为防护和个人信息保护等新要求，

6．调整了标准结构，将安全管理中心从管理层面提升至技术层面。

二、产品架构



dbAudit 系统运作架构包括 SecuCenter、SecuEyes、SecuAgent 及 SecuLog。

1．SecuEyes 主要负责采集与解析服务器的访问活动，并将收集的数据传输到 SecuCenter。

2．SecuCenter 采集与处理从 SecuEyes 传送过来的数据，将处理过的数据存储到 dbAudit 数据库中，用于分析与统计之用。为用户提供图形界面来查看、配置、管理用户的审计行为。

3．SecuAgent 用于采集经由 TCP 联机方式对服务器进行的访问活动，及在本机执行的 SQL 活动，并将采集的信息传送到 SecuCenter 或 SecuEyes。

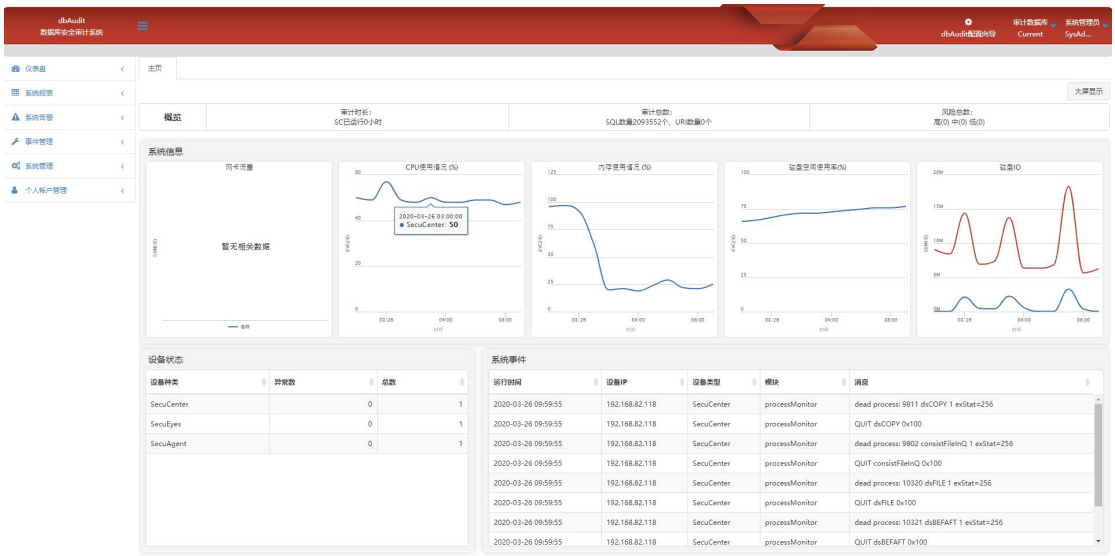
4．SecuLog 主要是定期备份 SecuCenter 的历史审计数据、报表和图表模板等备份数据。

三、产品特性

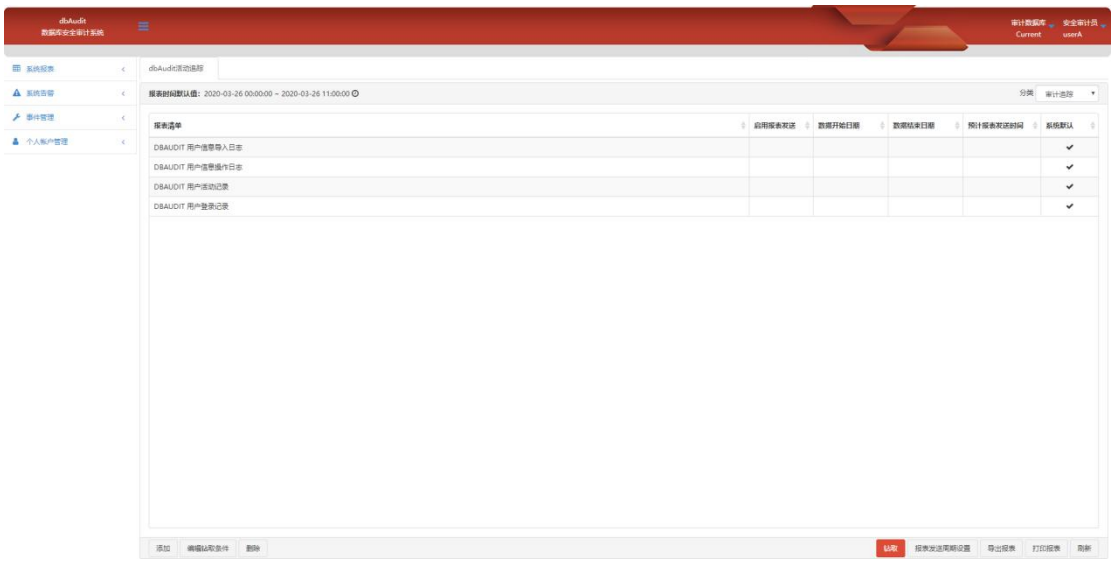
3.1 可靠的责任追溯机制

1．权责分离：账户角色规划防止滥权，适应对敏感内容审计的管理要求。角色划分为系统管理员，安全审计员，安全管理员，用户管理员，安控管理员五种权限职责划分。

1) 系统管理员：负责管理 dbAudit 系统和环境配置、监控系统运行状况和处理系统事件通知。

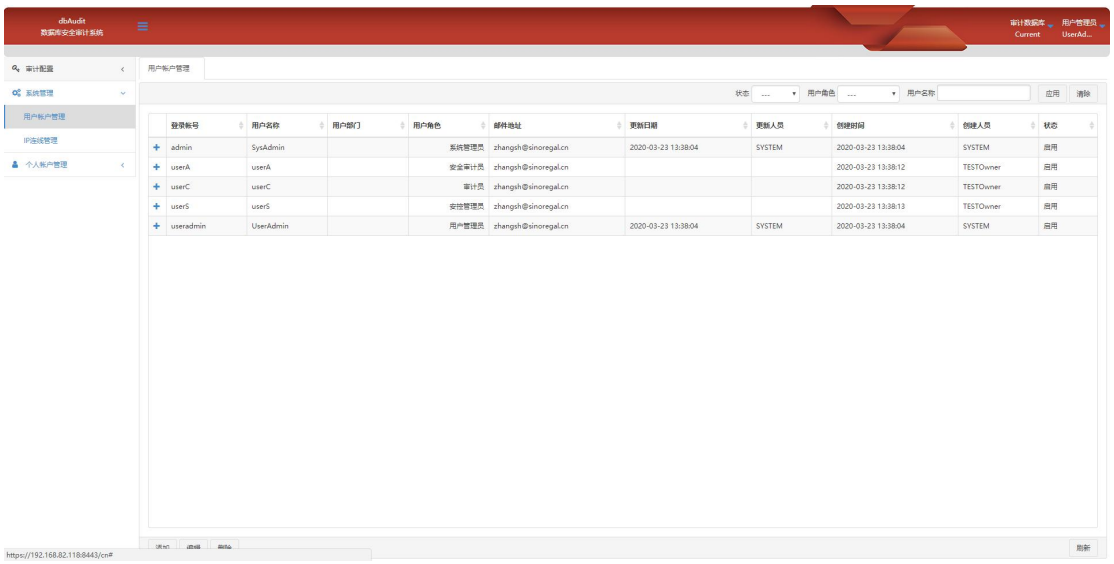


2) 安全审计员：主要通过报表、图表和告警来审计 dbAudit 的用户访问活动，以及处理 dbAudit 审计事件通知。

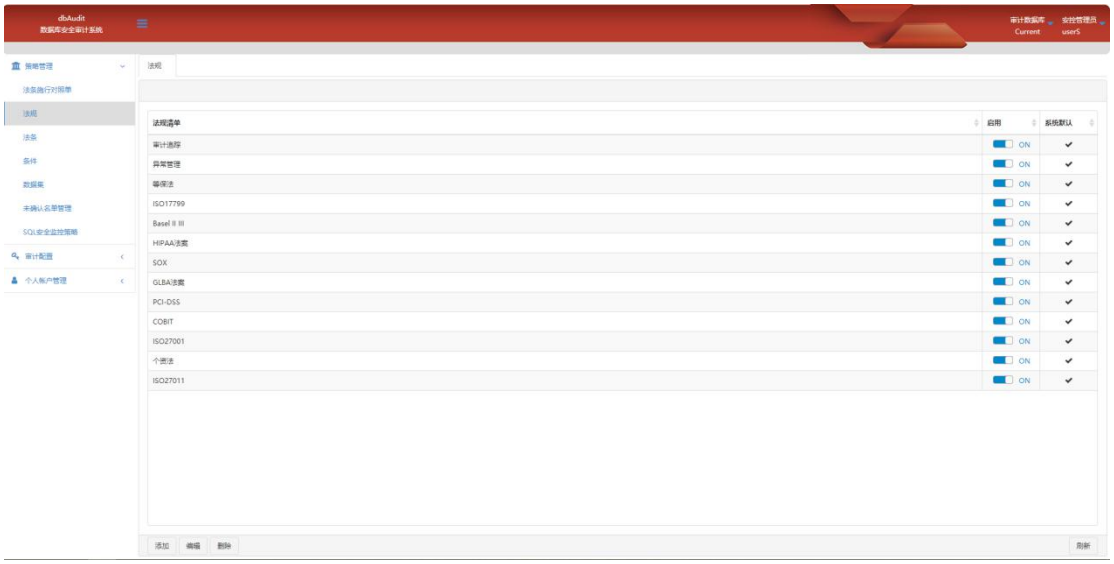


3) 审计员：主要通过报表、图表和告警来对监控目标上的数据访问活动执行审计任务，以及处理审计事件通知。

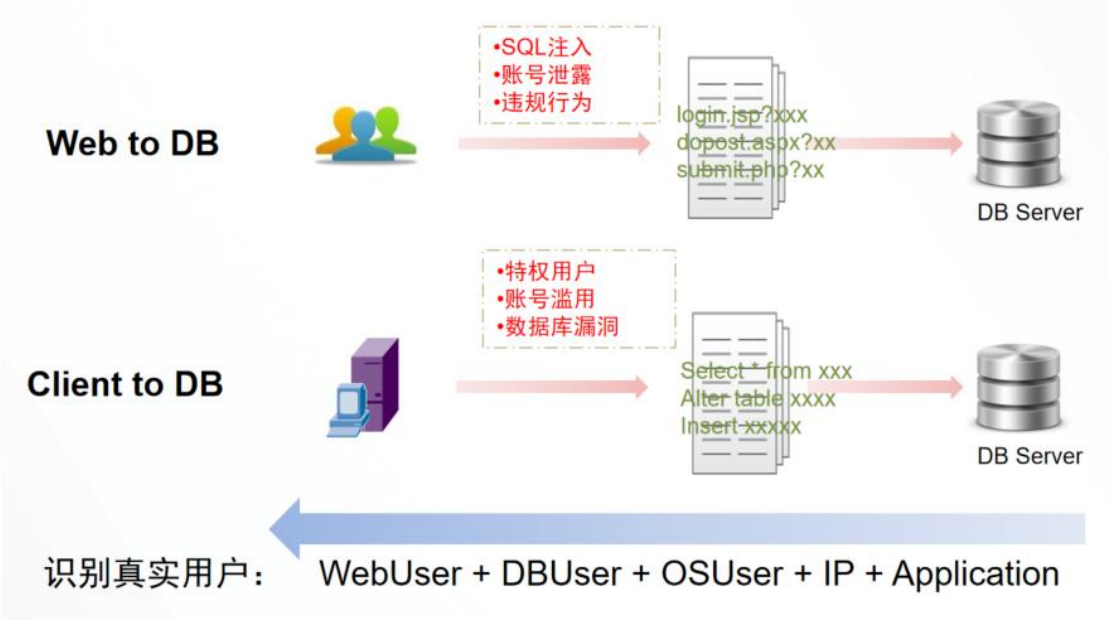
4) 用户管理员：负责管理用户、授予用户审核权限和指定各角色允许登录的位置，以及配置事件通知的审核流程和知会人员。



5) 安控管理员：主要负责审核策略相关项目的管理与设置。



2．端对端全程审计记录，精准定位风险源头，精准识别操作对象，精准关联风险线索。



3.2 违规行为自动预警

1．灵活定制告警策略：对于恶意的 SQL 注入行为、非法的业务登录、高危的 SQL 操作和过量的数据下载等各种违规行为，系统可以基于灵活的策略配置，设置风险规则，提供的风险告警。

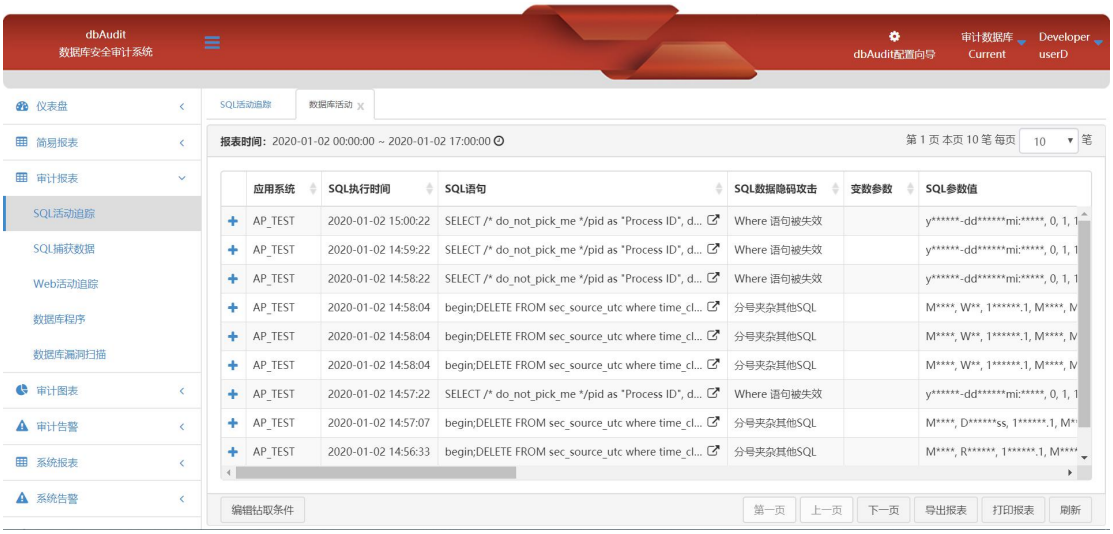
2．多种告警方式：dbAudit 的告警发送可以用 email，短信发送，亦可通过 Syslog 或 SNMP 方式发送给安全管理中心接收软件与安管平台整合。

3．事后处理：系统除了事中告警并记录违规行为，用户还可在事后进行事件管理：告警事件是否得到有效解决和重视。

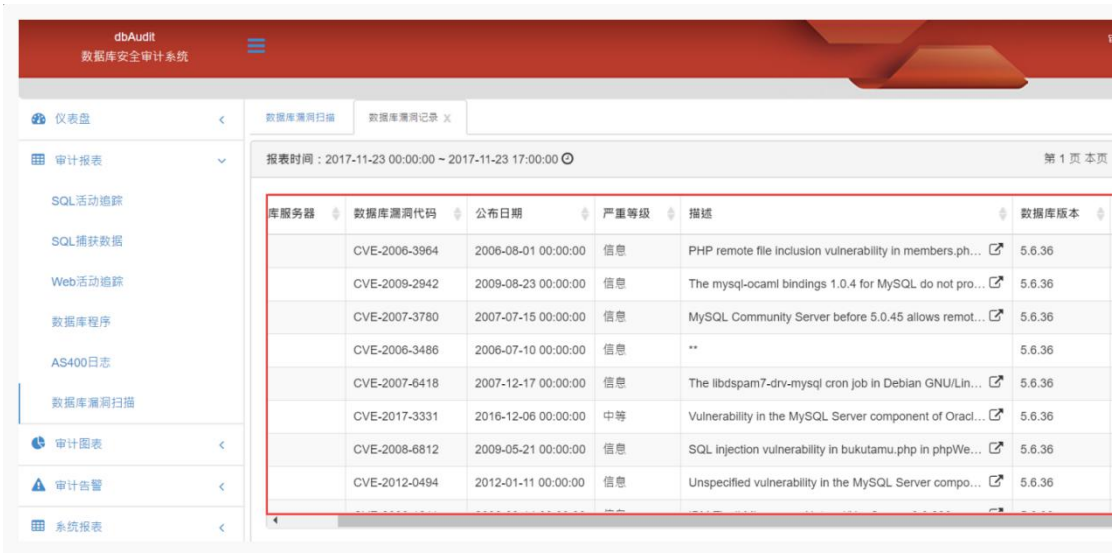
3.3 主动防攻击和防漏洞的方向转变

为了跟上用户对数据库安全的需求速度，dbAudit 已经不仅限于审计，而是向主动防攻击和防漏洞的方向转变。

1．系统自动生成 SQL 注入攻击报表



2．系统主动进行漏洞扫描



3.4 自动生成专业的合规性报告

通过汇总分析用户访问数据库行为，自动帮助用户事后生成合规性报告，满足用户的日常审计汇报、异常行为风险上报等需求。报告类型包括：

1．审计综合分析报告：基于审计信息进行审计日志的全量综合分析，全方位体现访问数据库行为状况。

2．合规性等保法报告：参考《中国国家信息安全保护检验标准》

完成设计，针对国家等级保护的检测要求进行审计数据统计梳理。旨在帮助数据库管理人员、审计人员对各种异常行为和违规操作及时发现，快速定位分析，为整体信息安全管理提供决策依据。

3．系统运行报告：汇总展现周期内产品的 CPU、内存使用趋势，及各存储分区使用情况，帮助用户了解产品资源使用状态，关注产品运行的稳定性。

4．系统用户异常行为分析报告：统计周期内，是否有非工作时间登录审计设备，并记录其最早登录时间和最晚登录时间。

5．自定义报告：用户可基于报表模型，自定义生成符合自身业务关注点的报表。

3.5 业务标签建模

目前市面上主流审计产品的审计结果为 SQL 语句，这需要相关的安全和数据库知识才能了解其含义。dbAudit 通过对业务标签的建模，使审计结果简单易懂，更贴近非 IT 专业人员的使用体验，扩大产品使用群体。

四、产品优势

4.1 强大的大型数据处理性能

dbAudit 具备对多种主流数据库的封包快速、高效、正确的解析、处理、入库能力：

1．客户案例：云南电网超高数据交易量级下 Oracle 解析协议

正确率受到客户肯定 (ie. 50000+ SQL/sec)。

2．支持数据库类型及版本

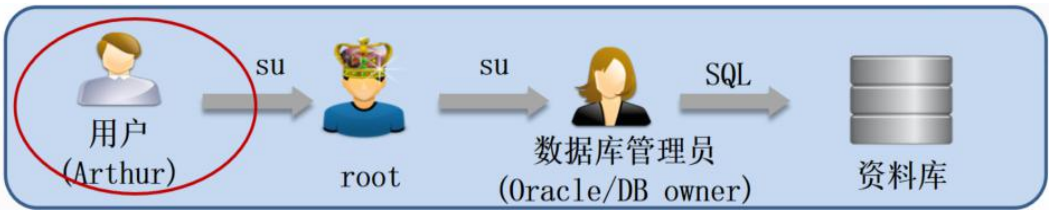
数据库	版本
Oracle	8i, 9i, 10g, 11g, 11gr2, 12c
MS SQL	2000, 2005, 2008, 2008R2, 2012
Informix	7, 8, 9, 10, 11, 11.5, 12 以上
DB2	8, 9.1, 9.5, 9.7, 10.5
Sybase	12.x, 15.x
MySQL	4.1 以上
PostgreSQL	8.3.4 以上
MongoDB	0.8 以上

4.2 用户真实身份认证

在 Web N-tier 应用架构下，目前大部分的数据库审计产品无法在不改应用的前提下辨识终端真实用户身份，但对于信息安全事件而言，讲究的是人+事+时+地+物的时间记录，所以终端用户真实身份便十分重要。

dbAudit 自行研发的网络用户身份认证技术（Web User Identification），使客户无需改变网络与系统架构，无需修改应用程序，即可辨别终端应用系统用户的真实身份及其存取数据库的行为。

➢ 用户隐藏身份时，执行记录应可分辨真实原始用户



➢ 执行记录应可分辨是否为自动程序（cron job）或是人为执行

➢ 执行命令信息应完整记录（程序名称与 OS 指令）

4.3 强有效的审计日志防护能力

多重审计日志防护，确保审计记录不被篡改，强化证据力：

1．dbAudit 审计数据备份文件均会加密压缩，并加注电子数字签名，防止审计数据被窜改。

2．dbAudit 审计资料无法被篡改，dbAudit 仅提供管理者通过浏览器接口（Web GUI）或 CLI（Command Line Interface）进行管理维护等工作，无法进入操作系统层，防止审计记录被篡改。

3．自我监测功能：dbAudit 仅提供用户查询审计轨迹纪录，无异动/删除功能，任何 dbAudit 操作行为系统均记录

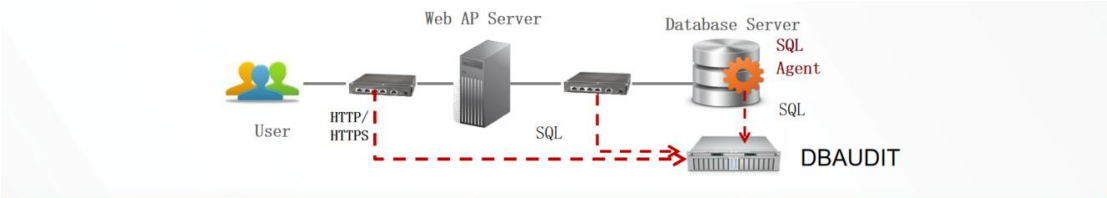
4.4 弹性架构，部署灵活

dbAudit 采用旁路镜像与本机端代理程序混合模式：

1．采用旁路方式抓取数据，对应用目标运行零影响。且此系统的部署与运作，完全无需启用数据库本身的审计记录日志(Audit Trail)功能或依赖数据库本身的日志记录。

2．混合模式：Network Sniffer 监控网络 Users+Agent 监控主机端特权用户,可将效能影响降到最低。

3．高效的代理程序（Agent）部署可以完美做到云环境下的审计：在云平台环境下网路的流量近乎不可能旁录出来审计，在此前提下可以安装高效能代理程序在云上的数据库端做到审计。



	旁路镜像	本机端代理程序	混合模式
网络应用系统用户	Yes	Yes	Yes
特权使用者/ 数据库主机端监控	No	Yes	Yes
效能影响	完全不影响数据库主机效能	流量大时, 将严重影响数据库主机效能	1. Network Sniffer监控网络Users 2. Agent监控主机端特权用户 3. 可将效能影响降到最低

五、产品环境

硬件平台

- CPU：Intel（8 核以上）
- Memory：16GB 以上
- HDD：1TB 以上

软件平台

- 操作系統：CentOS 6 （已内含在 Sinoregal dbAudit 安装文件）

六、我们的优势

6.1 技术优势

星瑞格的核心研发团队来自原 Informix 国内、外团队，团队成员

具备多年的专业经验，对数据库内部结构深度了解，掌握了数据库关键核心技术：

- 专注在数据库安全的技术研发和相关服务；
- 新增国产加密算法，满足国标加密标准，符合国家安全等级保护要求；
- 与国产服务器、国产操作系统、国产中间件做过适配与优化；
- 拥有自主研发的数据库复制产品(SinoRepl)、数据库安全审计产品（dbAudit)、数据库性能监控工具(dbSonar)等，逐步扩大了 SinoDB 的生态环境。

6.2 服务优势

星瑞格软件技术支持秉承以专业团队提供专业服务的理念，为用户提供基于项目前期的规划设计服务、项目中期的建设实施服务、项目后期的运营管理服务，以及在成熟环境中的优化提升服务，优势体现在：

- 集中了全亚太区的多位近 20 年专注于数据库安全的高级技术人员；
- 具备服务大型客户经验的专业团队，已提供 PICC、兴业银行、福建农信、大连银行、成都农信等银行的运维和研发服务；
- 构建了完善的技术服务流程，遵循专业的服务体系和质量体系，为客户提供优质、高效、主动、迅速的专业技术服务，服

务内容主要涵盖以下几个方面：

- ✧ 日常技术支持服务（5x8 服务）：日常邮件或电话支持服务、远程登录技术支持服务。
- ✧ 紧急故障排除服务（7x24 服务)：配置专门技术负责人员，提供故障排除服务；紧急情况下的短时间响应； 紧急故障排除服务报告；故障级别分类服务。
- ✧ 现场技术支持服务：包括系统规划、产品安装、产品升级、系统巡检、补丁维护、平台迁移、故障分析、数据迁移、数据备份、灾备机制建立与演练、性能测试及调优、系统安全建议、专项技术讨论、健康检查服务等。

七、典型案例

7.1 案例一、北京电网与云南电网公司数据库审计解决方案

7.1.1 面临问题

电网核心数据库面临“越权使用、权限滥用”安全威胁，以及需要满足法规对数据库审计的要求，因此部署数据库审计系统帮助电网解决下列问题：

- ➢ 自动识别数据库越权使用、权限滥用；
- ➢ 跟踪敏感数据访问行为，及时发现敏感数据泄漏；
- ➢ 发现 SQL 注入攻击；
- ➢ 满足法律、法规要求，提供合规报告。

避免电网内部员工发生越权使用，误操做，将重要数据删除，造

成营运异常，通过数据库审计，可以避免内部员工提权，当有提权行为时，可以立即发现通报管理员，阻止提权，避免误操作所带来的损失。

避免黑客入侵电网系统或内鬼配合入侵后，勒索电网公司，通过数据库高危指令，破坏系统营运，造成巨大损失，可以通过发现 SQL 注入攻击，提早发现系统遭遇入侵攻击，也可以通过发现越权，提权行为，提前发现系统异常。

电网系统存在大量客户敏感信息需要保护，当发现有高频次或大量访问敏感信息时，存在数据泄露风险，可能是外部黑客，也有可能是内鬼，因此通过数据库审计，可以发现是否有异常访问行为，追踪敏感数据访问轨迹，阻止数据泄漏，避免造成伤害与损失。

7.1.2 解决方案

1. 避免电网内部员工发生越权使用，误操做，将重要数据删除，造成营运异常：当有提权行为时，系统可以立即发现通报管理员，阻止提权。

2. 电网系统存在大量客户敏感信息需要保护：系统可以发现是否有异常访问行为，追踪敏感数据访问轨迹，阻止数据泄漏。

3. 避免黑客入侵电网系统或内鬼配合入侵后，通过数据库高危指令，破坏系统营运或勒索电网公司：

1） 系统可以通过发现 SQL 注入攻击，提早发现系统遭遇入侵攻击

2）通过发现越权，提权行为，提前发现系统异常。

4.针对等保法等测评要求：系统自动生成等各类合规性报表：自动记录数据库访问行为日志,追查有据，符合法规要求

7.1.3 实施成果

- 自动发现异常告警通知，提早发现，避免问题发生；
- 自动记录数据库访问行为日志，追查有据，符合法规要求；
- 自动生成等保法规要求报表。

7.2 案例二、福建星云云安全审计系统

7.2.1 面临问题

政务系统云数据库部署在云端，系统运维管理委托外包厂商管理。因职务排班轮调，有多位系统运维管理员，所以需要解决以下问题：

1.政务系统中经常会有数据共享，数据交换的功能操作，共享链条上的每一个节点，都有可能发生事故，而一旦发生数据泄漏密，追责、定责给政府部门带来了巨大的困惑

2.监管所有审计系统运维人员的操作行为，避免越权操作、数据泄漏等违规行为发生

3.政务系统数据在云上，面临着相关法规的要求：必需采取监管记录网络运行状态、并规范日志留存不少于六个月；等保法规亦要求上信息系统进行安全审计、安全控制

7.2.2 解决方案

1. 系统自动对所有数据库操作行为监控并记录，可以溯源追查，厘清责任。

2. 每日自动生成运维人员操作行为记录报表，监控操作行为,保留操作日志记录。

3. 系统可针对不同的法规法条进行定制报表，满足不同行业客户的需求。

7.2.3 实施成果

- 能够发现违规操作，进行追溯；
- 合理合规的多样化报表呈现审计结果。

7.3 案例三、福建国网数据库审计解决方案

7.3.1 面临问题

该项目经过前期的建设，设备、服务、中间件和应用系统的数据每年以成倍的速度增长，系统响应效率急需提高。目前无法记录并稽核所有造访数据库的存取轨迹，对追踪终端使用者的真实身分更是无从谈起。随着业务系统权利的外放及电子文件传递工具的发展，系统数据的保护日趋重要，对数据库敏感数据的安全方面监控管理功能需求尤为突出。因此部署数据库审计系统，期待解决以下问题：

1. 因国网项目建设过程中有多位系统运维管理员以及外包厂商，需要监管审计这些运维人员与外包人员的操作行为，避免越权操作。

2. 避免数据泄漏等违规行为发生。

3. 稽核所有造访数据库的存取轨迹，追踪终端使用者的真实身分。并记录操作行为，厘清责任

7.3.2 解决方案

1. 特权用户与外包商受到监控与管理

2. 敏感表格访问记录报表与大量敏感数据访问告警

3. 每日自动生成运维人员操作行为记录报表，监控操作行为，保留操作日志记录，可以溯源追查，厘清责任。

7.3.3 实施成果

- 能够长期保存操作日志记录，方便客户对历史数据进行审计；
- 对未知的潜在危险进行捕获，增加安全性。

7.4 案例四、福建省国资委数据库审计解决方案

7.4.1 面临问题

为实现“一中心一平台”的建设目标，“先平台、后应用、急用先行、逐步推进”的建设思路,为实现国资监管资源整合和信息共享，实现省属国资系统的监管业务协同。而数据库产品及安全审计产品作为监管数据中心的核心和基础，其重要性不言而喻。

因该信息系统将所有出资企业信息进行整合和共享，内有大量客户敏感信息需要保护，需要关注以下问题：

1. 是否存在高频次或大量访问敏感信息时，

2. 是否存在数据泄露风险

3. 需要避免内部员工越权访问等

7.4.2 解决方案

1. 识别越权使用、权限滥用，管理数据库帐号使用权限

2. 跟踪敏感数据访问行为，及时发现敏感数据泄漏

3. 生成敏感数据高频与大量访问报表

7.4.3 实施成果

- 每日自动生成符合等保法规要求报表；
- 每日自动生成运维人员操作行为记录报表，监控其操作行为；
- 每日自动生成客户敏感信息高频次与大量访问报表，发现异常。

7.5 案例五、福建省电子信息集团信息化系统

7.5.1 面临问题

近些年来快速发展，为了不断的提升集团的核心竞争能力，配合集团规模化的快速发展，集团引进了信息化的管理，建立独立于互联网的相关应用系统，为提高工作效率，各部室日常办公均在办公自动化系统上开展，部分上网信息不符合保密要求，存在涉密信息管理不规范问题。

为满足**信息系统安全等级保护三级要求建设**，保证数据库信息的安全，部署数据库审计系统。所有访问云平台内的数据库系统通过虚

拟机网络的旁路镜像流量到安全审计设备，在不影响受监控数据库性能和不改变应用架构情况下，实现真正全程范围无死角的端到端审计。

7.5.2 解决方案

1. 识别越权使用、权限滥用，管理数据库帐号使用权限

2. 捕捉到真实的数据库用户

3. 跟踪敏感数据访问行为，及时发现敏感数据泄漏

将前端真实用户与 WEB 操作进行关联

7.5.3 实施成果

- 每日自动生成符合等保法规要求报表；
- 每日自动生成运维人员操作行为记录报表，监控操作行为,保留操作日志记录,可以溯源追查，厘清责任。