官 网: b.360.cn 传 真: +86 10 5682 2000
北京市 朝阳区酒仙桥路 6 号院 2 号楼 100015

360 数据库审计系统

产品白皮书

March 2, 2017

目录

1.产品概述

360数据库审计系统是针对网络访问数据库的操作行为进行细粒度分析的安全设备，它可提供实时监控、违规响应、历史行为回溯等操作分析功能，是满足数据库风险管理和内控要求、提升内部安全监管，保障数据库安全的有效手段。

2.产品特点

2.1 专业的数据库审计

360 数据库审计系统能够对业务网络中的各种数据库进行全方位的安全审计，具体包括：

1)数据访问审计：记录所有对保护数据的访问信息，包括文件操作、数据库执行 SQL 语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息

2)数据变更审计：统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据

3)用户操作审计：统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断

4)违规访问行为审计：记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警

2.2 业务操作实时回放

360 数据库审计系统产品能对访问数据库操作进行实时、详细的监控和审计，包括各种登录命令、数据操作指令、网络操作指令，并审计操作结果，支持过程回放，真实地展现用户的操作。

借助360独有的基于会话的行为分析(Session-based Behavior Analysis)技术，审计员可以对当前网络中所有访问者进行基于时间的审查，了解每个访问者任意一段时间内先后进行了什么操作，并支持访问过程回放。真正实现了对“谁、什么时间段内、对什么（数据）、进行了哪些操作、结果如何”的全程审计。

2.3 事件精准定位

在信息安全及虚拟化背景时代下，单靠某一个信息去定位违规操作者已经成为不可能，如内网用户大多采用 DHCP 分配 IP 地址，没有做 IP-MAC 绑定及相应的准入规则，用户可通过更改操作系统名、IP 地址、MAC 地址等方式逃避追踪，传统的数据库审计定位往往局限于IP地址和MAC地址，很多时候不具备可信性。因此只有通过关联尽可能多的身份定位信息进行定位以及做一定的准入权限设置，其审计结果才具有可靠性，才能作为电子证据。360 数据库审计系统产品可以对 IP、MAC、操作系统用户名、使用的工具、应用系统账号等一系列进行关联分析，从而追踪到具体人。

2.4 事件关联分析

360 数据库审计系统产品可对响应事件进行关联，如根据 IP 关联出某段时间内该 IP 所触发的告警数量等；根据一段时间内的数据库或应用系统登录失败次数判断出暴力破解密码的可能性；根据账号的多次登录判断账号信息泄密或共享账号的可能性；相似 SQL 语句执行时间过长从而判断该语句设计的合理性等。根据事件关联性分析，自动涌现一批对客户具有实用价值的信息，帮助客户管理和维护好现有应用。

2.5 访问工具监控

360 数据库审计系统产品自动扫描连接数据库的访问工具。从访问数据库的源头进行分析，应用系统和客户端工具根据不同的数据库类型可通过 ODBC、JDBC、直连等方式连接数据库，直接连接工具如 Winsql、PLsql 以及 C/S 架构的客户端工具等。如发现审计记录中出现未知的数据库连接工具或出现规定之外的连接工具，审计员可根据工具监控记录分析出使用过该工具的 IP 及关联的操作记录，

进而取证使用该工具的源头及操作的合法性。

2.6 黑白名单审计

360 数据库审计系统产品可根据客户意见及实际审计情况，将 IP、操作语句、账号登相关信息加入黑白名单。同时，在应用系统中，因应用系统对应后台的 SQL 语句固定，一旦发现其中含有危险信息则可将对应的 SQL 加入黑名单，而一旦应用系统中有某些语句疑似风险操作但其实际并不产生危害则可加入白名单。

2.7 变量审计

在不同数据库及应用系统中，很多值的传递都是通过变量进行，如在 oracle 数据库中有绑定变量，在其它数据库中也有变量一说。如审计不到变量则无法对 SQL 指令的危险性进行判断。SecFox 安全审计系产品可对不同数据库的不同变量进行审计

2.8 关注字段值提取

360 数据库审计系统产品可根据配置，自动提取 SQL 指令中某关键字段的值，如查询语句中涉及的时间范围、查询的条件。由其是在金融、高值耗材等信息中，可通过查询条件查询出财产、费用、联系人等敏感信息，通过提取关注字段的值，并通过该值设置规则，则可更精确的对数据库访问操作进行精确审计。

2.9 丰富完善的报表报告

360 数据库审计系统内置大量报表报告，包括等级保护报表、数据库报表等。系统生成的报表图文并茂。报告可用 PDF、DOC、XLS 等格式存档。

3.产品价值

3.1 未知数据库资产发现

通过数据库审计产品的扫描功能，主动发现未知的数据库以及访问采用的应用程序，记录客户端的访问情况，帮助用户实现对网络中数据库资产的有效管理，避

免管理缺失造成的安全问题

3.2 敏感数据信息管理

通过数据库审计产品的使用，发现当前网络中存在的敏感数据信息，以及了解哪些数据信息需要管理和保护，进一步建立数据信息保护策略，避免数据信息泄露造成的不良影响

3.3 数据库安全事件预警

通过对数据库访问行为的监控审计，结合用户自定义的安全访问策略，实现对违规访问、越权使用、漏洞利用等非法访问行为的实时预警

3.4 数据库安全事件追溯

针对网络中数据库访问行为进行审计，详细记录数据库访问工具，以及整个访问过程，并实现对记录内容的关联分析，当发生安全事件时，可以帮助用户快速准确的定位事件源和整个访问过程，实现安全事件的可追溯。

3.5 辅助用户数据库访问策略制定

通过对网络中数据库访问行为的记录、审计、关联分心，为用户提供不同视角，不同维度的的数据库访问报表，未用户数据安全保护策略的制定提供数据支撑。

3.6 满足用户合规需求

针对等保/分保，以及一些行业性的审计需求，提供了专业的报表以帮助用户满足合规需求

4.主要功能

项目	分项	详细描述
产品功能	审计范围	包括 MS SQL Server、Oracle、DB2、Sybase、Mysql、Informix、达梦、Cache 在内的多种数据库
		包括 FTP、Telnet、HTTP 等协议
		采用独立的标准机架式硬件架构，软硬件一体化系统 采用全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统

	数据库审计	审计数据库的 DDL、DML、DCL 和其它操作等行为，审计内容可细化到库、表、记录、用户、存储过程、函数等
		支持数据库绑定变量审计
		支持端口重定向的审计
		支持超长操作语句审计，针对传统型数据库，支持 3 万字节的审计而不截断，针对 Cache 数据库，支持 50 万字节长度不截断
		支持 Cache 数据库集成工具 terminal、portal、studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 sql 语句、查询 Global、返回结果，Terminal 能审计到 M 语句和返回结果
		中间件的支持，支持 COM、COM+、DCOM 组件
		支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警
	规则管理	系统自带审计规则库，用户可自定义审计策略
		可提供通过子对象模式多级关联跨表跨字段的组合规则
		审计策略支持 select、create、execute、insert、alter、call、update、drop、logout、delete、rollback、login、truncate、grant 等数据库操作命令作为分项响应条件
		审计策略支持数据库语句执行时间、语句执行回应、最大操作语句长度等作为分项响应条件
		审计策略支持数据库客户端操作系统主机名及用户名、客户端进程、客户端 MAC、客户端 IP 等作为分项响应条件
		审计策略支持数据库名、表、包、过程、函数、视图、字段、索引、数据库帐户（用户名）等作为分项响应条件
		审计策略支持数据库操作返回内容、返回行数作为分项响应条件

		审计策略支持数据库操作关键字作为分项响应条件
功能展现	报表展现	包括数据库、等级保护等报表
		报表生成可日程规划，报告可用 PDF、XLS、DOC 等格式存档
	过程回放	数据库操作支持过程回放，展现用户操作
	隐秘设置	审计结果隐秘设置，通过*号对审计结果中的重要信息进行隐秘处理，防止非法权限查看
系统管理	自身监控	系统自身的健康状况监控，包括 CPU 和内存利用率等，遇到问题自动报警，确保安全管理平台自身的可靠性
		系统操作都记录日志并进行持久化存储，便于追踪、审核和告警
		系统日志格式的属性包括：时间、源 IP、用户名、操作类型、操作说明、操作结果
	自身安全	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
		系统本身具备能发现未知仿冒进程工具、防范非法 IP 地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能
		管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等
		能够对连续失败登陆进行自动锁定，锁定时间可设置
事件响应	告警配置	规则制定支持设定审计的触发条件和触发审计后的自动响应动作
	响应管理	告警支持发送邮件、SNMP Trap、Syslog、短信平台等响应动作
部署管理	部署方式	支持旁路部署，设备本身运转与否都不影响网络的正常工作
	管理模式	界面 100%都是 B/S 模式，全中文界面，安全 HTTPS 访问管理中心