腾讯数盾 数据安全审计 CDS-Audit

技术白皮书

目录

[第1章 系统概述 1](#_Toc512264734)

[1.1 背景 1](#_Toc512264735)

[1.2 简介 2](#_Toc512264736)

[第2章 产品功能 4](#_Toc512264737)

[2.1 人工智能威胁识别 4](#_Toc512264738)

[2.2 CVE规则库威胁识别 4](#_Toc512264739)

[2.3 自定义规则审计 4](#_Toc512264740)

[2.4 风险报表 4](#_Toc512264741)

[2.5 语句压力预警 4](#_Toc512264742)

[2.6 业务审计 4](#_Toc512264743)

[2.7 运维审计 5](#_Toc512264744)

[2.8 自定义报告 5](#_Toc512264745)

[2.9 等级保护报告 5](#_Toc512264746)

[2.10 威胁告警 5](#_Toc512264747)

[第3章 技术特点 6](#_Toc512264748)

[3.1 训练有素的AI引擎 6](#_Toc512264749)

[3.2 性能优异的高并发审计引擎 6](#_Toc512264750)

[3.3 严谨的三权分立 6](#_Toc512264751)

[3.4 重点突出的合规性报告 6](#_Toc512264752)

[第4章 适用行业 8](#_Toc512264753)

[4.1 金融、政府等保合规 8](#_Toc512264754)

[4.2 社交、游戏网站个人信息泄露定责 8](#_Toc512264755)

[4.3 医疗防统方 8](#_Toc512264756)

[4.4 企业数据被黑后取证 8](#_Toc512264757)

[4.5 各类应用系统的数据库安全审计 8](#_Toc512264758)

# 系统概述

## 背景

随着社会信息化深度日益加深，企业IT系统飞速扩张，线上的业务数据也越来越多。业务数据上线可以带来长久稳定的存储模式、快速高效的企业数据分析等各方面的好处，但同时也使得集中化的数据暴露在了恶意攻击、黑客渗透、内部泄密等风险之中。近几年频频发生公司因数据丢失受到重大损失的新闻，以及各类数据窃密的刑事案件，都是数据安全问题的真实写照。信息化系统中常见的数据风险主要有以下几类：

（1）数据系统分散，缺乏集中审计监控

各办公系统、企业网站均配置独立的数据库，系统分散、缺乏集中化管理。各个数据库虽然也有自己的日志，但受制于软件本身的设计，各数据库可提供的日志信息层次不齐，数据内容无法统一。如果有个别数据库没有配置日志相关选项，还会导致审计出现盲区。集中监控缺乏所导致最严重的问题在于，各数据库访问行为之间无法做到关联分析，对全局数据安全态势没有整体了解，这将会给信息系统管理带来非常大的隐患。

（2）恶意攻击日趋隐蔽，难以有效发现并制定应对措施

技术的发展不仅给安全防护措施带来了提升，攻击手段也因此受益而产生了质的飞跃。传统的脚本小子已经升级为有一定编程能力的黑客，被发现的各类恶意工具现在也很少有人直接使用。“0 day攻击”、“变种木马”现已成为各类信息安全新闻里的常客。当下变幻莫测的攻击手段中，传统的安全措施已经很难进行抵御。很有可能发生数据库已经被人攻破，黑客已经在源源不断的拿取企业数据，而企业还浑然不知的情况。如果这种情况发生，企业辛辛苦苦创造的各种营销数据、行业经验、技术积累，全部都成了他人的嫁衣。

（3）内部防范措施不到位，内网人员有机可乘

无论是云上还是云下，内部网络相比外网边界而言，都不得不更讲究效率而非安全。因此，内部如果出现有恶意行为的人员，将更容易轻车熟路的绕过安全系统，对数据库进行非法访问。此时，如果没有专业的数据安全审计系统辅助，不仅无法有效追查“内鬼”，而且无法形成有效的威慑力，使得有想法的人都会跃跃欲试。

（4）数据库压力监控不到位，突发性能问题

系统安全是一个广泛的概念，除了常见的黑客攻击、病毒感染等信息安全类型的问题，系统因配置过低、访问压力过大、网络流量过多而导致的宕机等事件，也是数据安全的一大隐患。数据库语句压力监控不到位，性能状况掌握不及时，通常是数据库宕机的主要诱因。而突发的宕机问题，将会严重影响企业信息系统的正常运行。

（5）获取泄密证据困难

企业发生重大泄密后，往往面临取证困难，无法为事件溯源等问题。即便泄密人员能够根据经验大致定位出来，也会因为缺少必要的证据而导致不能追究责任。与此同时，涉及公众影响的泄密事件，法律法规还有严格的日志存留期限要求，如果没有相应的审计措施，企业本身还将受到法律的追责。

## 简介

针对上述数据安全问题，腾讯数盾数据安全审计 CDS-Audit 能够在云上、云下环境任意部署，对企业网络中的数据库各类会话信息、访问操作、SQL语句进行全量审计入库。

获得审计数据后，CDS-Audit能够根据多种规则库和威胁检测引擎来识别操作中的恶意行为，并且及时通知管理员进行相应的安全防护措施。CDS-Audit还能够对数据库进行逐台的语句压力统计，通过历史纵向压力信息和数据库之间的横向压力对比展示各数据库的压力情况，协助管理员提前预防性能问题。对于已发生的安全事故，CDS-Audit支持在十数年的审计日志中检索蛛丝马迹，为企业还原安全事故的全貌并定位责任人。

数盾数据安全审计具备强大的AI威胁检测引擎，即使面对非常严峻的安全环境，CDS-Audit依然能够轻松预测变化，将各类新出现的变体攻击通报给管理员，帮助企业从容应对各种形态的攻击。

同时，CDS-Audit也能够应对因数据访问量巨大而产生的审计难题。数盾数据安全审计每秒SQL吞吐量达十万级，每小时入库速率达千万级，完美应对超高并发环境，在高强度语句压力面前数据不丢包，内容不失真，完整记录数据库访问信息。

# 产品功能

## 人工智能威胁识别

依托腾讯云专业的深度学习技术和丰富的样本训练环境，数盾AI引擎能够应对变化多端的攻击场景，对各类变体攻击以及非常见威胁操作实现监控。在数据攻击日益多样化的今天，CDS-Audit将为数据库安全提供更为精准的威胁分析和告警。

## CVE规则库威胁识别

结合即时安全情报，CDS-Audit具备强大的CVE引擎，能够根据威胁攻击、恶意操作、SQL注入的流量特征对安全事件进行告警。

## 自定义规则审计

支持按照库、表、字段、访问源、数据库实例等多种维度进行审计规则设置，安全策略灵活且自由，实现精细化监控；可根据不同场景不同类型的应用进行个性化定制，精确掌控数据库访问信息。

## 风险报表

整合CVE引擎、AI引擎、自定义规则库的监控信息，将全网数据库风险按照高、中、低三类详尽的展示在数据库管理员面前。风险可视化效果直观，内容简单易懂，能够辅助管理员全面掌握安全信息，为数据安全建设提供有力依据。

## 语句压力预警

数盾数据安全审计能够基于动态的会话信息整合成实时语句压力报表，从网络层面为管理员提供数据库语句压力概览。为网络中各数据库性能问题提供预测情报，辅助管理员优化相关业务性能。

## 业务审计

在业务审计方，数盾数据安全审计具备全量的会话审计功能，超越传统安全审计概念，将数据库所有的SQL操作全部收入眼底。会话审计类别齐全，存储周期满足合规性要求，能够为各类数据操作行为进行详细溯源，为数据库安全事件提供便利的追责效果。

## 运维审计

CDS-Audit不仅能够审计业务系统与数据库之间的操作，而且能够对负责数据库日常运维的DBA进行审计。审计内容包括登录时间、所用账户、SQL语句类型、SQL内容等信息，确保DBA的行为在受控范围内。

## 自定义报告

周期性的统计报告有利于提高管理员对全局安全信息的掌控力度。数盾数据安全审计支持20+的报告内容，并且可以自由组合，精准提供管理员在日常管理过程中所需的安全信息。

## 威胁告警

CDS-Audit能够在威胁操作被识别的瞬间，通过告警向相关管理员发送操作的源IP、所用账户、操作语句等各项信息。告警方式支持微信告警、短信告警、邮件告警、语音广播告警，类型丰富，多种途径确保警报及时通知管理员。

# 技术特点

## 持续进化的AI引擎

随着攻击技术的进步和黑色产业链的发展，任意小规模组织即可发起APT攻击、编写变种木马以及挖掘系统漏洞。这种变化使得信息安全形势变得越来越严重，传统的基于安全信息库的防御手段已经变得日益落伍。因为根据特征来识别威胁的安全库只能够在威胁爆发后才能发现此类威胁，而无法提前预测威胁发生的可能，2017年4月爆发的WannaCry能够迅速攻破全球数百个企业，就是因为它的特征没有被收录在案所致。

数盾数据安全审计依托腾讯强大的安全背景，AI引擎深度学习样本量级达到千万。通过高强度的样本训练，CDS-Audit能够精确识别各类变种攻击，将未爆发或者未收录到安全信息库的新型攻击手段进行识别。实现变种攻击预警的效果。

## 性能优异的高并发审计引擎

数盾数据安全审计具有高性能网络引擎和SQL语句分析引擎。秒级吞吐量可达数万条SQL，每小时入库速率可达千万级别，使得CDS-Audit在高并发环境下表现优异。与此同时，数十亿条在线SQL语句存储能力可让CDS-Audit轻松在海量数据中进行检索与分析，有效还原数据库安全信息。

## 严谨的三权分立

作为专业的信息安全产品，数盾数据安全审计具备强大的自身安全体系。除自我安全防护能力出众外，CDS-Audit还具有严格的账户管理体系，系统管理员、审计管理员、操作审计员三权分立，相互制约，确保您的安全管理工作从内而外的稳定。

## 重点突出的合规性报告

数盾数据安全审计能够满足等级保护在数据安全和信息审计方面的要求。在满足这些条例合规性的同时，CDS-Audit能够将所有相关的审计数据整理成报表，在一份报告中统一体现，让企业管理者对自身单位的合规性一目了然，确保心中有数。

# 适用行业

## 金融、政府等保合规

金融、政府等有严格法律法规要求的行业，CDS-Audit能够按照标准要求，提供完全对应条例的审计信息，确保网络合规性。

## 社交、游戏网站个人信息泄露定责

社交、游戏等具有公民个人信息的网络服务商，在发生个人信息泄露时，如果不能在刑事调查过程中配合司法部门进行取证和定责，可能会有连带责任。CDS-Audit能够追溯信息泄露事件，确保网络服务商不受牵连。

## 医疗防统方

卫计委明确要求各大医院开展防统方工作，杜绝医疗回扣。CDS-Audit行为分析功能可精准定位统方操作，有效威慑统方人员，满足医院响应卫计委管理制度的需求。

## 企业数据被黑后取证

企业的营销信息、产品价格等重要数据被竞争对手窃取后，往往因为审计不力，证据不足等问题导致无法追责。CDS-Audit强大的日志检索能力可为信息泄露事件取证，帮助企业追回损失。

## 各类应用系统的数据库安全审计

数据是各类企业、政府信息系统最重要的资产之一。因此，数据安全也是各行各业需要重点关注的目标。CDS-Audit适用环境广泛，审计能力优异，能够在各行各业数据库系统中发挥安全作用，提升企业数据安全能力。