

DSP数据库审计管理平台



产品概述

迪普数据库审计管理平台 (DPtech DSP) 是一款全新研发的企业级数据安全审计产品。集多核并行处理、精准协议解析、海量日志存储和检索等技术于一身, 为用户提供完整的数据库审计分析、泄密轨迹分析、数据库攻击威胁分析等安全能力, 有效帮助用户实现事件追根溯源, 全面保护数据资产安全。

产品特点

全面审计、防止漏审

可通过主机探针技术对数据库行为进行流量捕获, 从而实现了数据库访问流量的全方位监控。

精准识别、准确解析

基于精确 SQL 语句协议识别、解析和三层关联技术, 提供更准确的数据库审计记录, 为可信审计溯源提供了坚实的基础。

高效存储、快速分析

创新的采用非结构化的存储方式, 1T 硬盘可以存储15亿到 20 亿条日志; 同时配合海量日志存储分析检索技术, 实现了亿级数据的秒级检索和分析。

日志脱敏、简单易用

提供业务翻译能力, 便于非专业人员查看, 可以用其它内容或符号代替日志中存在的敏感信息, 防止敏感数据的泄露。

产品系列



DSP1000 数据库审计管理平台

功能价值

产品功能	功能价值
数据库兼容性	支持 Oracle、MSSQL、DB2、Sybase、Informix、MySQL、人大金仓、神通、达梦、南大通用、HANA、HWMPP、HighGo、Hive、MongoDB 等主流数据库
审计粒度	依照 5W 原则--Who、Where、When、How、What，全面记录对数据库服务器的连接情况、会话相关的各种信息和原始 SQL 语句。包括数据库实例、数据库类型、数据库用户、操作系统用户、主机名、数据库 IP、客户端 IP、数据库 MAC、客户端 MAC、客户端程序、客户端用户名、客户端端口、捕获时间、执行时长、动作、日志级别、风险等级、告警规则、SQL 内容等
三层关联审计	三层关联审计，能够实现完整的业务审计。可以完成从真实用户访问应用程序、应用程序访问数据库之间的行为进行关联。能够将真实用户计算机 IP 地址、登陆的用户名、数据库 IP地址、SQL 语句、访问发生的时间等信息记入审计日志，从而定位到网络中具体的人，实现全方位的审计
超长语句审计	支持跨包的 SQL 语句拼接功能，能够完整解析与审计超长 SQL 语句，屏蔽逃逸审计通道
入侵检测	可以对网络中存在的 SQL 注入、缓冲区溢出、权限提升等漏洞攻击行为进行审计和告警。

产品功能	功能价值
日志模糊化	用其它内容或符号代替日志中存在的敏感信息（如身份信息、联系方式），在日志存储和检索过程中显示模糊化后的内容
日志报表	具备强大的报表模板以及可定制的客户化报表，满足不同层次用户的需要。可提供 DPA、SOX、等保、医疗防统方等行业性报表模板
三权分立	采取三权分立的账户管理模式，实现安全管理员，系统管理员与安全审计员权限分离，满足相关法律法规要求
专用软硬件平台 **	采用飞腾CPU、盛科交换芯片的专用硬件平台，软件平台拥有麒麟内核使用授权

**此特性仅在特定款型支持

杭州迪普科技股份有限公司

地址：浙江省杭州市滨江区通和路68号中财大厦6楼

邮编：310051

官方网站：www.dpotech.com

服务热线：400-6100-598

杭州迪普科技股份有限公司 保留一切权利

免责声明：虽然 DPtech 试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，为此 DPtech 对本资料中信息的准确性不承担任何责任。DPtech 保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。