LanSecS®
莱 恩 赛 克
www.sbr-info.com

LanSecS®
数据库安全防护系统

北京圣博润高新技术股份有限公司
BEIJING SBR HIGH-TECH CO.,LTD

LanSecS® 数据库安全防护系统

传统网络防火墙已无法阻挡由数据库系统自身缺陷和应用层SQL协议引入的安全风险。

数据库系统存在的安全风险

分 类	风险名称
授权管理	滥用过高权限
	滥用合法权限
	身份验证不足
攻击类	数据库平台漏洞
	操作系统漏洞
	SQL注入攻击
	拒绝服务攻击
	权限提升
	通信协议漏洞
审计类	审计记录不足
加密类	库明文数据暴露

数据库系统自身安全缺陷

分 类	缺陷名称
数据库系统漏洞	拒绝服务漏洞
	缓冲区溢出
	系统注入漏洞
	权限提升漏洞
访问控制缺陷	超级用户不受限
	SQL注入漏洞
	SQL特征控制
	高危SQL控制
	数据无返回数量控制
明文存储	数据明文存储
	日志明文存储
	备份明文存储
	配置文件暴露密码

产品介绍

圣博润LanSecs数据库安全防护系统，是基于数据库协议分析与控制技术，实现对数据库操作“危险指令阻断、访问行为控制、安全态势分析、全面行为审计”的数据库安全主动防御产品。

功能特性

虚拟补丁

➤ 在数据库系统外的网络层创建了一个安全层，在用户无需真实补丁的情况下，阻断利用漏洞的攻击行为，完成对数据库漏洞的安全保护。规则库跟随 CVE升级，已支持 22类，460个以上虚拟补丁。

SQL注入禁止

➤ 通过对SQL语句进行注入特征分析，完成对SQL注入行为的检测和阻断。系统提供缺省SQL注入特征库，同时提供定制化的扩展接口。

黑白名单

➤ 通过学习模式捕获以及SQL语法抽象构建动态模型，形成 SQL语句白名单和SQL语句黑名单，放行 SQL白名单特征语句，阻断 SQL黑名单特征语句。

精细访问控制

➤ 提供比数据库系统更详细的虚拟权限控制；

➤ 控制策略包括：用户+ IP+MAC+应用程序+操作+对象+时间；

➤ 在控制操作中增加了Update Nowhere、delete Nowhere等高危操作；控制规则中增加返回行数和影响行数控制。

行为监控与审计

➤ 提供全面详细审计记录，告警审计和会话事件记录，并在此基础上实现了内容丰富的审计浏览、访问分析和问题追踪，提供实时访问仪表盘；

➤ 通过对捕获的SQL语句进行精细SQL语法分析，并根据SQL行为特征和关键词特征进行自动分类，系统访问 SQL语句有效“归类”到几百个类别范围内，完成审计结果的高精确和高可用分析。

实时安全态势分析

➤ 提供实时安全态势分析仪表板，漏洞攻击、SQL注入、高危操作、SQL吞吐量等数据图文并茂实时显示，而且可以自动生成报表并自动发送邮件。实时风险告警通知方式包括： Syslog、snmp、邮件、短信。

产品优势

高度适应性

➤ 系统支持多种主流数据库系统：Oracle、DB2、SQLserver、MySQL、Sybase、DM、KingBase、Gbase；

➤ 系统设计采用B/S架构，所有管理操作均使用浏览器完成，并且与管理机的操作系统和浏览器版本无关；

➤ 产品提供多档性能选择，满足用户环境多样性；

➤ 产品具备双机热备能力和后台数据自动备份功能，充分满足用户业务连续性高的要求。

高度应用兼容

➤ 对于IPS 类产品最重要的是在保持“低漏报率” 的同时维护“低误报率”；对于数据库而言这点更为关键，一点点“误报”可能就会造成重大业务影响；

➤ 系统提供强大的应用行为描述方法，以对合法应用行为放行，将误报率降低为“零”；

➤ 系统通过语法抽象描述不同类型的SQL语句，规避参数带来的多样化；通过应用学习捕获所有合法SQL的语法抽象，建立应用 SQL白名单库。

全面入侵阻断

提供业界最为全面的数据库攻击行为检测和阻断技术：

➤ **虚拟补丁技术：**针对 CVE 公布的漏洞库，提供漏洞特征检测技术和漏洞利用阻断技术；

➤ **高危访问控制技术：**提供对数据库用户的登录、操作行为，提供根据地点、时间、用户、操作类型、对象等特征定义高危访问行为；

➤ **SQL注入禁止技术：**提供SQL注入特征库；

➤ **返回行超标禁止技术：**提供对敏感表的返回行数控制；

➤ **SQL黑名单技术：**提供对非法SQL的语法抽象描述。

实时安全预警

➤ 安全态势分析功能使得数据库运行过程数据化、视觉化、可控制。同时也采用了多种技术手段满足产品自身安全需求。

快速部署实施

➤ 预定义策略模版：系统提供应用场景、维护场景、混合场景多种策略模版帮助用户快速建立安全策略；

➤ 预定义风险特征库：系统通过预定义风险特征库快速建立风险阻断规则；

➤ 多种运行模式：系统提供 IPS、IDS运行模式，提供学习期、学习完善期、保护期三种运行周期，以帮助用户在系统部署的不同阶段平滑过渡。

产品部署

串联模式

支持两种串联模式：

➤ 透明网桥模式：在网络上物理串联接入本系统，所有用户访问的网络流量都串联流经设备；通过透明网桥技术，不改动用户环境原有IP地址和参数；

➤ 代理接入模式：在网络上旁路接入本系统，修改数据库客户端地址逻辑连接本设备，本设备再转发流量到数据库服务器；通过代理接入模式，可以保持网络物理拓扑结构不变。

旁听模式

➤ 通过TAP设备或交换机端口镜像等技术将网络流量映射到本系统实现旁听接入；通过旁听部署模式不改变原有网络拓扑，但是对于高风险操作只能报警而不能阻断。

用户收益

➤ 合规达标，符合安全规范要求；
➤ 抗攻击抗抵赖，提高数据库应用的访问安全能力；
➤ 满足数据库数据“机密性、完整性、可用性”的安全要求；
➤ 提高业务连续性和灾备能力。

产品资质

➤ 公安部颁发的销售许可证
➤ 中国信息安全认证中心颁发的中国国家信息安全产品认证证书
➤ 国家保密科技测评中心颁发的涉密信息系统产品检测证书

产品规格表

防护系列

型 号	配 置	性能参数
LDB-F1000	1U,千兆电口 x6，1TB	1000条SQL/秒吞吐量不超过1000并发连接
LDB-F5000	1U,千兆电口 x6，2TB	5000条SQL/秒吞吐量不超过2000并发连接
LDB-F10000	2U,千兆电口 x6，3TB双电可扩万兆光纤口X2	10000 条SQL/秒吞吐量不超过4000并发连接
LDB-F30000	2U，千兆电口X6，4TB双电可扩万兆光纤口X2	30000 条SQL/秒吞吐量不超过8000并发连接

审计系列

型 号	配 置	性能参数
LDB-A1000	1U，千兆电口X6，1TB	1000条SQL/秒吞吐量不超过1000并发连接
LDB-A5000	1U，千兆电口X6，2TB	5000条SQL/秒吞吐量不超过2000并发连接
LDB-A10000	2U，千兆电口X6，3TB双电可扩万兆光纤口X2	10000条SQL/秒吞吐量不超过4000并发连接
LDB-A30000	2U，千兆电口X6，4TB双电可扩万兆光纤口X2	30000条SQL/秒吞吐量不超过8000并发连接
LDB-A50000	2U，千兆电口X6，4TB双电可扩万兆光纤口X2	50000条SQL/秒吞吐量不超过10000并发连接

北京圣博润高新技术股份有限公司
BEIJING SBR HIGH-TECH CO.,LTD
地址：北京市海淀区高梁桥斜街59号院2号楼3层 / 邮编：100044 / 电话：010-82138088 / 技术支持热线：8008102332/4009662332 / 技术支持邮箱：support@sbr-info.com / 网址：www.sbr-info.com