## 产品概述

数据库防火墙是继防火墙、下一代防火墙等网关类安全产品之后，专门针对于数据存储的核心介质——数据库的一款安全防护产品。目前数据库安全可以分为两个层面，一方面是来自于外部的威胁，比如说来自黑客的攻击、非法访问等，第三方运维人员的不当操作和非法入侵；另外一部分是来自于内部的威胁。这两个层面的安全威胁都需要针对数据库入口进行安全控制，提高数据应用安全性。

捷普数据库防火墙系统是一款主动的、实时的、基于数据库协议分析与控制技术的数据库安全防护系统。数据库防火墙部署于数据库之前。必须通过该系统才能对数据库进行访问或管理。

捷普数据库防火墙基于主动防御机制，除了提供网络防火墙的基本隔离功能以外，能够实现数据库的访问行为控制、危险操作阻断、可疑行为审计、数据库攻击防护、数据库状态监控、操作行为审计、综合报表等功能。

## 产品特点

* 保护数据库及核心数据安全

捷普数据库防火墙产品对数据库的高危操作进行事前预防，发现违规操作时实时阻断，事后通过综合审计能力提供详细的操作行为分析，从而可对数据库形成事前、事中、事后全方位的保护。

* 保护数据库免受攻击

数据库主要面临的攻击为缓冲区类攻击和SQL注入攻击，捷普数据库防火墙产品内置海量的攻击规则库，可以及时识别、发现针对数据库的攻击行为，并可对攻击行为进行阻断。从而保护数据库免受攻击，避免损失。同时详细的审计下攻击操作发生的时间、来源IP、登录数据库的用户名、攻击代码等详细信息。

捷普数据库防火墙产品自带虚拟补丁功能，在数据库外的网络层创建了一个安全层，用户在无需补丁情况下，完成数据库漏洞防护

* 防止内部高危操作

数据库系统维护人员包括运维管理员、外包人员、开发人员等，有些维护人员拥有直接访问数据库的权限，有意无意的高危操作会对数据造成破坏。

捷普数据库防火墙产品能够通过限定更新和删除影响行、限定无Where的更新和删除操作、限定drop、truncate等高危操作避免大规模损失。

* 满足合规/审计的要求

数据库系统维护人员在利益诱惑下，可能会通过业务系统提供的功能完成对敏感信息的访问，进行信息的售卖和数据篡改。

捷普数据库防火墙产品提供对所有数据访问行为的记录，包括用户名、IP地址、请求的数据库、连接建立的时间、连接断开的时间、通信量大小、执行结果等等信息。对风险行为进行SysLog、邮件、短信等方式的告警，并提供灵活的回放日志查询分析功能，大量内置报表及自定义报表的功能，提供详尽的事后追踪分析工具，可以满足客户合规和审计的要求。

* 细粒度数据库用户权限管理

捷普数据库防火墙产品在不影响数据库用户配置的前提下，对于当前数据库用户提供详细的权限控制，数据库用户访问数据库的行为受到系统的权限管理。捷普数据库防火墙能够根据用户/属性（IP/MAC）/时间等条件设置登录控制，还能够根据用户+操作+对象+时间等维度进行数据库控制策略；针对DCL/DML/DDL操作进行细粒度的操作控制；同时支持返回行数和影响行数控制。数据库用户权限的细粒度管理功能，避免数据库维护人员花费大量精力对数据库用户的权限重新调整，同时，避免了数据库用户权限滥用造成的数据泄漏等危险。

* 深度的安全评估功能

捷普数据库防火墙针对数据库漏洞进行检测、安全配置检查、补丁检查、缺省用户名/口令检查等，根据扫描结果输出漏洞检查报告，包括整体情况、漏洞详情、解决建议等。同时系统内置预定义评估策略，包括全面扫描、快速扫描（高、中风险）、CVE漏洞扫描、CNNVD漏洞扫描等多种策略供数据库维护人员选择。

## 产品功能

* 快速部署实施能力

捷普数据库防火墙内置预定义的安全策略模板，能够提供多种策略模版帮助用户快速建立安全策略。

捷普数据库防火墙支持数据库主动发现功能，能够按照地址范围、协议类型/端口，单次或定期（每日、每周、每月固定时间）发现网络中的数据库服务器，极大的提高维护实施进度。

捷普数据库防火墙支持控制和审计两种模式，控制模式支持监控并拦截威胁的拦截模式和监控，发现异常仅告警的监控模式。审计模式支持记录所有对数据库的访问的全部审计和只记录存在风险的访问行为的报警模式，可以由运维管理人员根据管理情况及时的调整部署模式。

* 全面的协议支持

捷普数据库防火墙支持多种数据库协议，如Oracle、SQLServer、DB2、Informix、Sybase、Cache、MySQL、PostgreSQL、达梦、GBase、金仓、Oscar、Teradata、MaxDB、Mongo等国内外主流数据库。

捷普数据库防火墙支持的运维协议包括SSH、Telnet、HTTP、FTP、SFTP、NetBIOS、NFS等。

* 细粒度访问控制

捷普数据库防火墙能够提供细致的权限控制功能，根据用户/属性（IP/MAC）/时间等条件设置登录控制，还能够根据用户+操作+对象+时间等维度进行数据库控制策略；针对DCL/DML/DDL操作进行细粒度的操作控制；同时支持返回行数和影响行数控制。

* 黑白名单支持

捷普数据库防火墙进行数据库防护的过程中，除了利用数据通讯协议解析的信息设置相应的风险拦截和违规sql操作预定义策略以外，还支持SQL白名单和SQL黑名单，对符合SQL白名单语句放行，对符合SQL黑名单特征语句阻断。

* 阻断和审计

捷普数据库防火墙产品具备全面的数据库审计能力，提供了全面详细的审计记录和丰富的告警，并在此基础上实现了内容丰富、动态可跟踪的实时审计分析和追踪。捷普数据库防火墙通过对捕获的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。

捷普数据库防火墙产品提供两种阻断动作，中断会话，断开数据库连接和拦截语句返回错误。

捷普数据库防火墙提供单向审计、双向审计、BS/CS三层环境用户审计等方式。

捷普数据库防火墙的告警通知方式包括syslog、snmp、邮件、短信和APP等多种方式。

* 行为监控与分析

捷普数据库防火墙能够提供全面详细审计记录，行为分析、风险分析和数据库监控，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，提供实时访问统计图。

* 数据库状态监控

捷普数据库防火墙能够实时监测服务器CPU、内存、磁盘等资源占用，实时监控服务器应用进程、业务端口、业务连接、流量变化等信息，当发现异常情况时，可及时向管理员预警，并可通过保护系统关停异常行为或异常连接，保障业务安全和服务可用性。

## 典型部署

捷普数据库防火墙产品具备串联和旁路两种接入模式。在串联模式下具备高效的阻断和审计能力，帮助用户实时阻断高风险行为，提高对数据库访问的可控度。同时还支持双机热备组网模式和硬件BYPASS。在旁路模式下具备详细审计能力，帮助用户及时发现针对数据库的高风险行为，并且用户可以从多维度了解数据库活动现状。

* 串联模式

当数据库防火墙产品串联到网络时，系统以控制模式运行，支持全部安全控制策略，可对被保护的数据库进行强访问控制、监控和审计。这种模式对来自网络的数据库操作进行很“强”的控制，可支持所有的安全控制策略。

* 旁路模式

当数据库防火墙采用旁路模式时，产品不直接接入网络，而是通过TAP、SPAN等技术将网络流量映射到数据库防火墙设备。旁路部署模式既不改变网络拓扑，也不在应用链路上增加新的设备点，避免单点故障的出现。