腾讯云T-Sec 云访问安全代理-数据安全防护 数据库加密服务

产品名称	腾讯云T-Sec 云访问安全代理-数据安全防护 数据库加密服务
公司名称	昆山昱唯网络科技有限公司
价格	3000.00/月
规格参数	品牌:腾讯云 产品:云访问安全代理
公司地址	花桥国际商务城曹新路70号
联系电话	17601404160

产品详情

购买流程：1.首先注册一个腾讯云账号：https://partners.cloud.tencent.com/invitation/1000028889485ab10aa8524fa （如已有腾讯云账号，请进入同意成为一下我们客户，我们将为您提供免费服务支持）。2.完成实名认证：https://console.cloud.tencent.com/developer/auth （公司使用，请完成企业实名认证，有部分产品，只能企业使用，能企业认证尽量企业认证，没法完成企业认证，请使用个人实名认证）。3.进入购买页面，即可购买使用：https://buy.cloud.tencent.com/casb什么是云访问安全代理云访问安全代理（Cloud Access Security Broker，CASB）是一款面向应用的数据防护服务，用免应用开发改造的配置方式，提供面向服务侧的字段级数据存储加密防护，有效防护内外部数据安全威胁。该服务已通过国家密码管理局的安全认证，满足商用密码应用安全性评估的相关合规要求。产品功能字段级加密CASB 提供可视化管理控制台，管理员可进行加解密权限规则的设置，颗粒度可以达到数据库表的字段级（如手机号）。对应用透明Proxy
对应用透明，不改变之前的运行机制，写入加密，读取解密。高可靠密钥管理数据加密密钥由腾讯云密钥管理系统（KMS）统一管理，密钥管理系统底层使用国家密码局或 FIPS-140-2 认证的硬件安全模块（HSM），并支持权限管控和内置审计，全方位保护您的密钥安全。灵活部署应用系统无需改造，用户只需配置数据库和 Proxy 的绑定关系，绑定后应用系统中的数据库地址和认证信息更改为 Proxy 的地址和认证信息，即可接入云访问安全代理。用户配置相应的加解密策略后，实时生效，就可以完成加密改造。大规模部署统一管控面对企业信息系统多、数据库多的情况，可部署统一云访问安全代理业务数据加密平台，进行集中管理。支持高可用CASB 支持高可用方式部署，支持主从互备模式，防止主机故障、网络故障或程序故障引起的业务损失。敏感数据识别云访问安全代理平台基于安全合规出发，保护数据的隐私及其安全性的要求，通过识别规则的设定、模式的匹配，自动扫描检测具有敏感数据的列表内容，并对其进行分级分类。数据脱敏通过对数据源配置脱敏规则，平台将依据规则实现敏感数据的脱敏，通过丰富的脱敏算法，进一步提高数据的安全性，确保敏感信息不易泄露。安全合规云访问安全代理支持国密算法（SM4）以及国际算法（AES），密钥由腾讯云 密钥管理系统（KMS）进行统一管理。服务已通过国家密码管理局的安全认证，满足商用密码应用安全性评估的相关合规要求。细致管控管理员可通过界面设置加解密策略，控制颗粒度可达到数据库的字段级（如手机号）。云访问安全代理数据库版的访问控制与数据库本身的访问控制独立，以此实现系统管理员、安全管理员和审计管理员的权限分立。高性能国密支持云访问安全代理提供高性能国密中间件，可以为企业应用提供高性能的 SM4 算法实现高速加解密，保障业务效率不受影响。高可靠密钥管理数据加密密钥由腾讯云密钥管理系统统一管理，

密钥管理系统底层使用国家密码局或 FIPS-140-2 认证的硬件安全模块（HSM），并支持权限管控和内置审计，全方位保护您的密钥安全。灵活部署面对企业信息系统多且数据库多的情况，云访问安全代理服务支持统一部署。应用系统无需改造，用户只需配置数据库和 Proxy
的绑定关系，绑定后应用系统中的数据库地址和认证信息更改为 Proxy 的地址和认证信息，即可接入云访问安全代理。用户配置相应的加解密策略后，实时生效，就可以完成加密改造。可用性保障云访问安全代理支持高可用方式部署，支持主从互备，进而防止主机故障、网络故障或程序故障引起的业务损失。云访问安全代理可适用于腾讯云内所有用户，是一款面向应用的防护服务，该服务用免开发改造的配置方式，快速解决用户加密需求，同时满足国密合规要求以及相关政策要求，帮助不同行业解决加密痛点问题。加密细控痛点：传统数据安全以基础设施为主，例如数据库加密
TDE、全磁盘加密等，防护粒度粗。 企业内部 IT 人员和外部黑客从服务侧窃取数据，访问敏感数据。方案：用户管理员可通过界面设置加解密策略，控制颗粒度可达到数据库的字段级（如敏感字段、手机号等）。使用云访问安全代理服务，实现从应用到数据库的控制范畴内，关键信息都是密文，密钥管理与密文数据分离，防护内外部威胁。快速部署痛点：通过开发改造应用，实现数据存储加密、动态访问控制。改造应用成本高、风险大且周期长。方案：面对企业信息系统多、数据库多的情况，云访问安全代理服务支持统一部署。用户只需配置数据库和 Proxy
的绑定关系，绑定后应用系统中的数据库地址和认证信息更改为 Proxy 的地址和认证信息，即可接入云访问安全代理。用户配置相应的加解密策略后，实时生效，就可以完成加密改造。支持的数据库类型及版本目前云访问安全代理仅支持 Mysql
5.6及5.7版本，暂不支持其他类型及其他版本数据库。对数据库字段类型的支持目前支持的数据库类型为Mysql，支持的字段类型如下：字段类型支持情况可选算法char支持51个及以内汉字支持155个及以内字母AES/SM4varchar支持AES/SM4tinytext支持51个及以内汉字AES/SM4text支持AES/SM4mediumtext支持AES/SM4longtext支持AES/SM4tinyblob支持AES/SM4blob支持AES/SM4longblob支持AES/SM4tinyint不支持-smallint不支持-mediumint不支持-int/integer不支持-bigint不支持-float不支持-double不支持-decimal不支持-date不支持-time不支持-year不支持-datetime不支持-timestamp不支持-对 SQL
语句的支持对数据库查询语句的支持情况如下：插入语句：类型支持情况SQL
样例不指定列插入支持insert into table_a values ('a',1,'bbb','ccc','ddd',3.74, sysdate);指定列插入支持insert into table_a(col1, col3, col4) values('a','bbb','ccc');删除语句：类型支持情况SQL
样例等值匹配删除，策略配置在其中某个条件字段上支持delete from table_a where col1='aaa' and col3='bbb';带 in 的删除，策略配置在 in 字段上支持delete from table_a where col1 in ('a','b','c');带子查询的删除，策略在子查询的条件字段上支持delete from table_a where col1 in (select col2 from table_b where col3 = 1);更新语句：类型支持情况SQL 样例策略配置在查询条件上支持update table_a set col1='aaa' where col2=1;策略配置在更新字段上支持update table_a set col1='aaa' where col2=1;查询语句：类型支持情况SQL 样例对 select * 语法的支持支持select * from table_a;条件字段等值匹配支持select col1 from table_a where col2=1;条件字段范围查询不支持select col1 from table_a where col1 > 'aaa' and col2 < 3;条件字段带函数不支持select col1 from table_a where substr(col1,0,2) = 'aa';条件字段带 in支持select col1 from table_a where col1 in ('a',b','c');SQL
语句中的表使用别名，选择字段及查询条件通过别名指定支持select t.col1 from table_a t where t.col2=1关联查询，策略在条件字段中支持select table_a.col2, table_b.col2 from table_a join table_b on table_a.col1 = table_b.col3 where table_a.col4='ccc'关联查询，策略在选择字段中支持select table_a.col2, table_b.col2 from table_a join table_b on table_a.col1 = table_b.col3 where table_a.col4='ccc'关联查询时使用 select *支持select * from table_a join table_b on table_a.col1 = table_b.col3 where table_b.col4='fff';选择字段带别名支持select col1 a, col2 b from table_a子查询-
简单语法子查询，策略在子查询条件语句上支持select col1 from table_a where col1 in (select col2 from table_b where col3 = 1)子查询-子查询中字段作为关联条件支持select a.col1 from table_a a join (select col2,col3,col4 from table_b) t on a.col1=t.col3 where t.col2='ddd'子查询-策略配置在子查询条件字段上支持select t.col4 from table_a a join (select col2,col3,col4 from table_b) t on a.col1=t.col3 where t.col2='ddd'子查询-
结果集中带有子查询字段，且配置了策略支持select t.col4 from table_a a join (select col2,col3,col4 from table_b) t on a.col1=t.col3 where t.col2='ddd'对 exist 关键字的支持支持select col1,col2,col3 from table_a where exists (select 1 from table_b where col3 = table_a.col1)对 group by 语法的支持支持select col1, col2 from table_a where col3 = 'bbb' group by col1,col2对数字类型的分组函数不支持select sum(col2),avg(col2),min(col2),max(col2) from table_a where col1='aaa'对 order by

的支持只支持非加密字段的排序select * from table_a order by id desc临时表支持select * from (select table1.col1,table1.col2,table1.col3,table2.id,table2.col4 from table1,table2 where table1.col1 = table2.col1) tmp其他注意事项数据库数据库、表和字段名不区分大小写。仅支持 utf8 和 utf8mb4 字符集。连接数据源删除后重新添加时，需要建立新的 MySQL 连接查询。连接内不允许切换登录用户。后端 DB 认证方式仅支持mysql_native_password和caching_sha2_password。不支持 SSL 连接, proxy 账号认证方式为mysql_native_password。加解密所有表结构必须预先在策略控制台定义，账号必须和相应数据源绑定后才能通过 proxy 操作相应的数据源。连接查询时，JOIN字段需选择同样的密钥，否则密文不一致，无法正确进行连接查询。不支持 变量的加解密。不支持 函数字段加解密。不支持 COM_QUERY 的 Prepare、Execute 语句的加解密。UNION 语句应用第一个 SELECT 语句的加解密策略。加解密前后字段值类型不能改变。ORDER BY， GROUP BY 不能用于加密字段。LIKE 条件不能用于加密字段。语句DML 执行前，需先切换到相应的库SET语句仅支持 SET NAMES utf8和SET NAMES utf8mb4, 其余的SET语句将被忽略。不支持 COM_STMT_SEND_LONG_DATA，COM_STMT_RESET 协议。不支持 COM_QUERY Protocol::LOCAL_INFILE_Data 协议。不支持 MultiResultSets 结果集处理。不支持 SELECT INTO 语句。不支持 mysqldump。不支持 INSERT VIEW，UPDATE VIEW，ALTER VIEW。不支持 CREATE TABLE xx AS SELECT、CHECK TABLE、CHECKSUM TABLE 语法。有包含 INFORMATION_SCHEMA 的语句都会忽略。其他数据库产品除了 TDSQL 增删改查语句的行首注释外，SQL 语句中的其余注释不会生效。TDSQL 的 ShardKey 字段不能配置加密。不支持 TDSQL自定义的管理语法, 如 help, repair 等。