炼石
CipherGateway

# 数据存储加密技术白皮书

北京炼石网络技术有限公司

Beijing Lianshi Networks Technology Co.,Ltd.

让数据共享更安全、更有价值

All for your service needs!

# 前言

十种数据存储加密技术白皮书

数据作为新的生产要素，其蕴含的价值日益凸显，而安全问题却愈发突出。而密码技术，是实现数据安全最经济、最有效、最可靠的手段，对数据进行加密，可在开放环境中实现数据的安全流转和使用。随着《密码法》等“一法三规一条例”的落实，各行业对数据加密技术、产品和服务的重视程度不断提升。

本文聚焦十种数据存储加密技术，希望能够帮助读者快速了解数据存储加密技术的全貌，并在客户需要通过“加解密技术”进行自身核心数据资产的安全保护时，在场景适用性判断、相关产品选型等方面提供有效的参考和帮助。

# 实战与合规双驱动



在“实战与合规”共同驱动下，数据安全建设作为“业务需求”逐步被重视，将与之匹配的安全技术应用到信息系统业务场景，迫在眉睫。

从实战化角度来看，当下的数据安全事件频发，面对全新的安全挑战以及新合规要求，企业安全体系正在从“以网络为中心的安全”，加速升级到“侧重以数据为中心的安全”。而密码作为网络安全的杀手锏技术和核心支撑，天然具备安全防护基因，是实现数据安全最经济、最有效、最可靠的手段。尤其在数字化政务、金融、教育、医疗、文旅、电信等行业，个人信息保护、商业秘密保护、国密合规等方面的建设亟待加速。

聚焦数据实际流转过程，在每个关键节点上，作为生产要素的数据都面临着众多威胁。通过对数据流转中的威胁分析，选取关键安全增强点进行加密，用这种方式给数据重新塑造了一个虚拟边界，实现防范内外部安全威胁，成为当前数据安全防护的主要手段。


图 1：基于数据流转路径的威胁模型分析

从合规性角度来看，数据安全技术迎来发展新趋势：第一，数据安全技术正逐步获得国家政策层面的重视以及用户应用层面的认可，从顶层设计到配套政策法规的不断加码，企业层面越发重视加密技术应用；第二，数据安全技术应用从通信安全等领域快速被扩展到各领域行业，如国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的发布，替代行标 GM/T 0054-2018《信息系统密码应用基本要求》，密码技术的行业及场景适用性进一步扩展延伸；第三，数据安全技术与业务的结合越来越紧密，业务应用层正成为数据安全建设的中心，将成为解决企业在平衡合规压力、改造复杂业务和信息系统困境的“钥匙”。

| 新合规政策条例 | | |
|---|---|---|
| 层级 | 名称 | 条例 |
| 国家顶层设计 | 《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》 | 第六部分“加快培育数据要素市场”第 22 条：**加强数据资源整合和安全保护。**推动完善适用于大数据环境下的数据分类分级安全保护制度，**加强对政务数据、企业商业秘密和个人数据的保护。** |
| | 《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》 | 第十八章第一节：**加快推进数据安全、个人信息保护等领域基础性立法**，强化数据资源全生命周期安全保护。第十八章第三节：**加强网络安全关键技术研发……** |
| 数据安全政策法规 | 《网络安全法》 | 第二十一条：国家实行网络安全等级保护制度。其安全保护义务第 4 条明确**采取数据分类、重要数据备份和加密等措施。** |
| | 《个人信息保护法（草案）》 | 第五十条第三款：**采取相应的加密、去标识化等安全技术措施；**<br><br>第六十二条：有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处**五千万元以下或者上一年度营业额百分之五以下罚款…** |
| | 《数据安全法（草案）》 | 第十九条：国家根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，**对数据实行分级分类保护。**<br><br>第二十五：**采取相应的技术措施和其他必要措施，保障数据安全。** |

| | | |
|---|---|---|
| 密码产业政策法规 | 《密码法》 | 二十七条：法律、行政法规和国家有关规定要求**使用商用密码进行保护的关键信息基础设施，**其运营者应当使用商用密码进行保护。关键信息基础设施运营者，**应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。** |
| | 《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号） | 第四章第三十条：各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，**按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。** |
| | 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020]1960 号） | 第二部分第六点：落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。**第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。** |
| | 《关键信息基础设施安全保护条例（征求意见稿）》 | 第四章第二十三条第四点：**采取数据分类、重要数据备份和加密认证等措施。** |
| | 《商用密码管理条例》 | 第六章第三十八条：非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，**其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，**自行或者委托商用密码检测机构开展商用密码应用安全性评估。 |

# 数据流转的安全增强点



数据安全本质上是由攻防对抗推动发展的，实战为加密技术的应用提供了内在需求，合规对加密技术的应用推广起到直接有效的手段，在实战与合规双驱动下，数据存储加密技术在业务中的应用成为技术大势所趋。

数据存储加密防护的难点，在于如何对流转中的数据进行主动式实施加密等保护，确保数据不被未授权篡改或泄露，这里的数据涵盖结构化与非结构化两种类型。结构化数据一般是指可以使用关系型数据库表示和存储，表现为二维形式的数据，本质来讲，结构化数据也就是传统数据库中的数据形式；非结构化数据，顾名思义，就是指没有固定结构的数据，包括各种文档、图片、视频/音频等，终端平台的很多重要文件、视频、图片等都属于这个范畴。

传统的“数据库加密”往往体现为密文数据存储到数据库后的情形，往往局限于结构化数据，而在企业实战化场景中，数据库却仅仅是数据处理的一个环节或载体，因此，传统的数据库存储加密技术是“数据存储加密”的子集。

针对加密技术对数据的安全防护，我们认为有四方面指标：第一，应满足加密防护能力融入业务流程，提供多场景细粒度有效防护；第二，能够融合访问控制、审计等其他安全技术，实现安全机制可靠有效运行；第三，优秀的权限控制能力，能够根据不同属性的人群，展开细致的权限控制，实现权限的最小化，有

效防范内部越权、外部黑客拖库等风险；第四，在节约企业成本，不影响企业业务正常运营的情况下，敏捷部署实施高性能的数据安全防护。而**在实际应用中，为了满足这些指标要求，需要对用户场景的适用性进行判断，并结合具体的场景化需求，选择一种或者几种的技术组合，优劣势互补，打造出“以密码存储技术为核心，访问控制、审计等多种安全技术相互融合”的数据安全防护体系，从而切实满足企业多场景的实战化及合规需求！**本文以“数据”为中心，沿着数据流转路径，在典型 B/S 三层信息系统架构的 10 个重要数据业务处理点基础上，综合业内数据加解密现状，选取了对应的 10 种代表性的存储加密技术，并对其实现原理、应用场景，以及相应的优势与挑战进行解读分析。


图 2：数据存储加密技术总览图

# 十种数据存储加密技术分析

全面、系统、多维度

## 技术一：DLP 终端加密

### 1）原理解析

**部署位置：**终端

**原理：**DLP（Data leakage prevention）终端加密技术，目的是管理企业终端上（主要指 PC 端）的敏感数据，其原理是在受管控的终端上安装代理程序，由代理程序与后台管理平台交互，并结合企业数据管理部门的管理要求，对下载到终端的敏感数据进行加密，形成适合企业的数据分级分类策略，从而将加密应用到企业数据的日常流转和存储中。信息被读取到内存中时会进行解密，被未授权复制到管控范围外则是密文形式，主要适用于非结构化数据的保护。

### 2）应用场景

DLP 终端加密技术主要适用于企业 PC 终端数据的安全管理，在原有安全防护能力之上，可有效增强以下场景的数据防护能力：

1）操作失误导致技术数据泄漏或损坏；
2）通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据；
3）离职人员通过 U 盘、CD/DVD、移动硬盘随意拷走机密资料；
4）移动笔记本被盗、丢失或维修造成数据泄漏。

### 3）优势

**1、外发交流安全可控。**终端加密主要适用于企业 PC 终端的场景，因此，经常会有“限制”合作方或外部人员使用企业文件　　相关权限的需求，DLP 终端加密可以顺利实现这个需求，从而保证外发交流文件的安全性。

### 4）挑战

**1、终端适配困难、运维成本高。**企业终端一般存在操作系统众多、终端类型复杂、文档使用场景又多样等情况，终端加密在落地应用时，易出现终端兼容适配困难、运维成本较高等问题。

## 技术二：CASB 代理网关

### 1）原理解析

**部署位置：**终端-应用服务器之间

**原理：**CASB 代理网关（Cloud Access Security Broker）是一种委托式安全代理技术，其核心利用 CASB 技术，将网关部署在目标应用的客户端和服务端之间，无需改造目标应用，只需通过适配目标应用，对客户端请求进行解析，并分析出其包含的敏感数据，结合用户身份，并根据设置的安全策略对请求进行脱敏等访问控制，可针对结构化数据和非结构化数据同时进行安全管控。

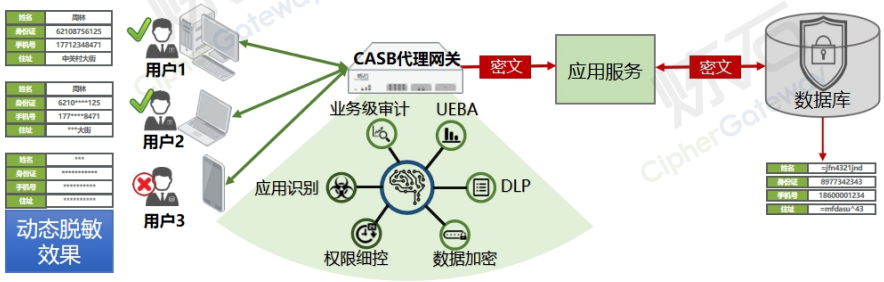


图 3：CASB 代理网关技术原理

### 2）应用场景

随着云技术和虚拟化技术的普及，传统的 IT 架构正在发生变化。企业很多业务系统都托管在云服务商处，日常的很多工作，比如 HR、社保、报销、OA 等工作事务的管理都有相应的 Saas 服务可以采用，企业想要享受便捷的云化服务，又不想失去对自身数据的控制权，则可以采用 CASB 代理网关技术。例如，最常见的一种安全防护场景是：能够识别出一个用户访问云资源是使用的私人账号还是企业账号，以防止敏感数据从企业资源转移到私人资源。

### 3）优势

**1、与业务结合的数据安全保护。**CASB 代理网关位于应用服务和用户端之间，独特的加密位置和加密形式，令该加密技术可以基于用户、资源、操作和业务上下文属性，灵活利用访问者所对应属性集合决定是否有权访问目标数据，比如部门、区域、职位、动作、目标数据类型、时间，以及其他条件等，从而实现基于复杂业务需求的对内容的安全防护；

**2、业务应用安全审计。**当企业对业务操作拥有复杂的审计需求时，可以使用该加密技术，CASB 代理网关能实现对业务操作进行独立且不可篡改的审计，如提交、审批、上传、下载、共享，以及对数据的增、删、改、查等，可实现对业务操作行为的异常发现、违规告警，帮助用户对安全事件进行追溯和定位。

### 4）挑战

**1、实施成本较高。**为实现从客户端请求中解析用户在应用中的操作含义，需适配目标应用，适配工作量会随目标应用的复杂度和安全管控力度增强而增加。

## 技术三：应用内加密（集成密码 SDK）

### 1）原理解析

**部署位置：**应用服务器

**原理：**应用内加密（集成密码 SDK）是指应用系统通过开发改造的方式，与封装了加密业务逻辑、实践模型以及设计模式的密码 SDK 进行集成，并调用里面的加密接口，使目标应用系统具备数据加密能力。

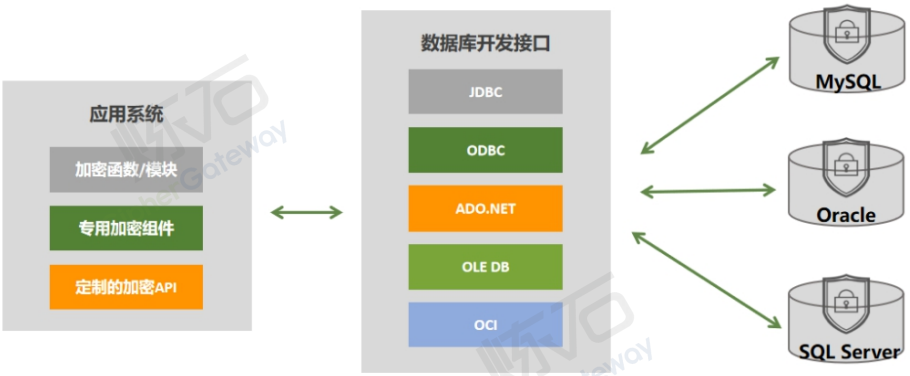


图 4：应用系统加密技术原理

### 2）应用场景

通常情况下，当应用系统仅对有限/使用频率较低的敏感数据存在加密需求时，比较适用于使用应用内加密（集成密码 SDK）技术。这里主要包含两种场景：第一，需要加密处理的敏感数据对应的表或字段相对较少；第二，需要加密处理的敏感数据在整个业务系统中使用相对不多。

### 3）优势

**1、适用范围广。**应用系统的开发商可以自行解决数据加解密的所有问题，对数据库系统本身或第三方的数据安全厂商没有依赖；

**2、灵活性高。**应用服务端加密，主要指针对于应用服务器的加密方式，因为应用服务端加密可与业务逻辑紧密结合，在应用系统开发过程中，灵活地对相关业务中的敏感数据进行加密处理，且使用的加密函数、加密密钥等均可以根据业务逻辑需求进行灵活选择。

### 4）挑战

**1、需要对应用系统开发改造。**应用系统加密的实现需要应用系统开发投入较大的研发资本，同时也需要较高的技术复杂度，造成实施和维护成本增加，有可能影响业务的正常开展；

**2、应用开发人员密钥使用不合规。**在实际应用中，会出现应用开发人员密钥使用不合规等情况出现，从而造成一定的数据安全风险。

## 技术四：应用内加密（AOE 面向切面加密）

### 1）原理解析

**部署位置：**应用服务器

**原理：**应用内加密（AOE 面向切面加密）技术，**能以免改造方式，实现应用系统中结构化数据和非结构化数据的存储加密，并提供细粒度身份访问控制、多种脱敏策略及审计功能，为应用打造全面有效且易于实施的数据安全保护。**其实现原理是将数据安全插件部署在应用服务中间件，结合旁路部署的数据安全管理平台、密钥管理系统和数据审计分析系统，通过拦截入库 SQL，将数据加密后存入数据库。

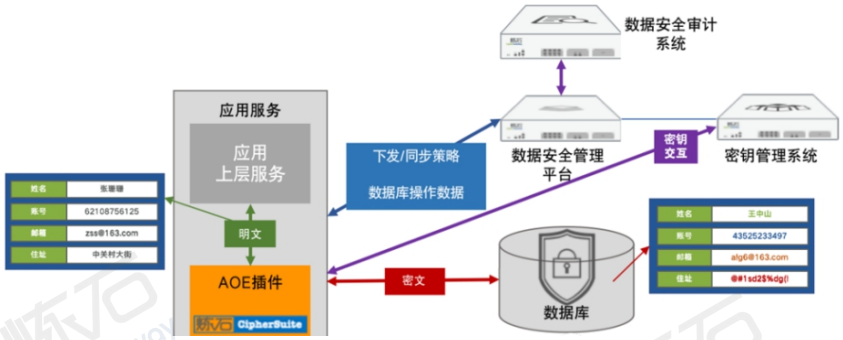


图 5：应用内加密（AOE 面向切面加密）技术原理

### 2）应用场景

应用内加密（AOE 面向切面加密）主要适用于企业在应用层想要实现免开发、低成本、高性能的数据安全防护。该加密方式支持结构化/非结构化数据的加密，可与应用开发解耦，拥有高灵活性。另外，该加密方式可支持分布式部署，集中管理，可针对单个应用防护，也可以针对几十个应用的批量保护。

### 3）优势

**1、基于细粒度权限控制的数据安全防护。**该加密技术适用于针对应用打造“主体到用户，客体到字段”的安全防护体系的场景化需求，该加密技术能够根据不同属性的人群，展开细粒度的权限控制，实现对企业内部人员的敏感数据访问最小化授权；

**2、业务和安全解耦。**该加密技术通过 AOE 面向切面加密方式，可以将安全与业务在技术上解耦，又在能力上融合交织，拥有高度灵活性；

**3、敏捷部署，对业务运营无影响。**应用内加密（AOE 面向切面加密）适用于“应用免改造”的实战需求，虽然是应用内加密的一种，但却能够实现以配置的方式敏捷部署实施，对应用的连续运行无影响。

### 4）挑战

**1、对应用程序编程语言和框架需要做适配。**企业实际应用系统错综复杂，涉及到多样化的编程语言与框架，这对 AOE 面向切面加密技术的实现提出较高的工程化实现挑战。

## 技术五：数据库加密网关

### 1）原理解析

**部署位置：**应用服务器-数据库之间

**原理：**数据库加密网关是数据库前置代理加密的一种，通过部署在应用服务器和数据库服务器之间的代理网关设备，解析数据库协议，对传入数据库的数据进行加密，从而获得保护数据安全的效果。

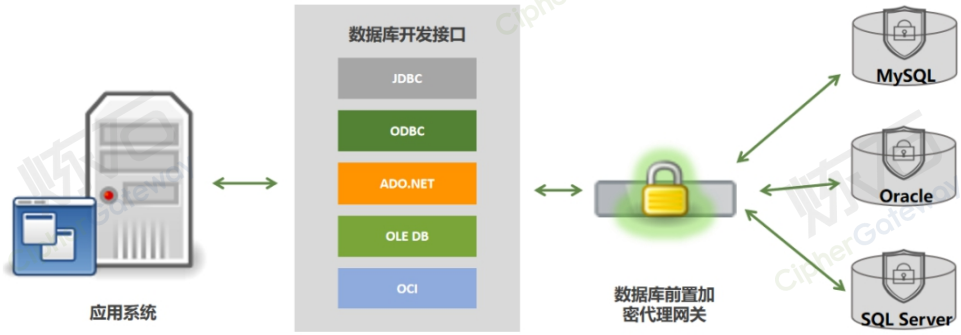


图 6：数据库加密网关技术原理

### 2）应用场景

数据库加密网关可以为数据库提供实时防护，本质上类似于为数据库提供了一个防火墙。可以建立数据库用户的访问控制，实现企业内部人员的敏感数据访问授权精细化，可以防数据库拖库以及拦截非法 SQL。

### 3）优势

**1、应用系统与加解密功能分离。**相比较于传统的应用内加密（集成密码SDK）技术，数据库加密网关技术因为它的独立性，能够使最终用户从高度复杂且繁重的加密、解密处理逻辑的开发工作解放出来。

### 4）挑战

**1、性能较低。**数据库加密网关因为吞吐量和处理能力有限制，导致处理速度较慢，不适用于一些高并发的应用系统或场景；

**2、存在一定的法律风险。**对于Oracle这类不开源、采用私有协议的商业数据库，安全厂商提供的数据库加密网关破解协议的方案存在法律风险。

## 技术六：数据库外挂加密

### 1）原理解析

**部署位置：**数据库

**原理：**数据库外挂加密通过针对数据库定制开发外挂进程，使进入数据库的明文先进入到外挂程序中进行加密，形成密文后再插入数据库表中。这种技术使用“视图”+“触发器”+“扩展索引”+“外部调用”的方式实现数据加密，可保证应用完全透明。通过扩展的接口和机制，数据库系统用户可以通过外部接口调用的方式实现对数据的加解密处理。视图可实现对表内数据的过滤、投影、聚集、关联和函数运算，在视图内实现对敏感列解密函数的调用，实现数据解密。

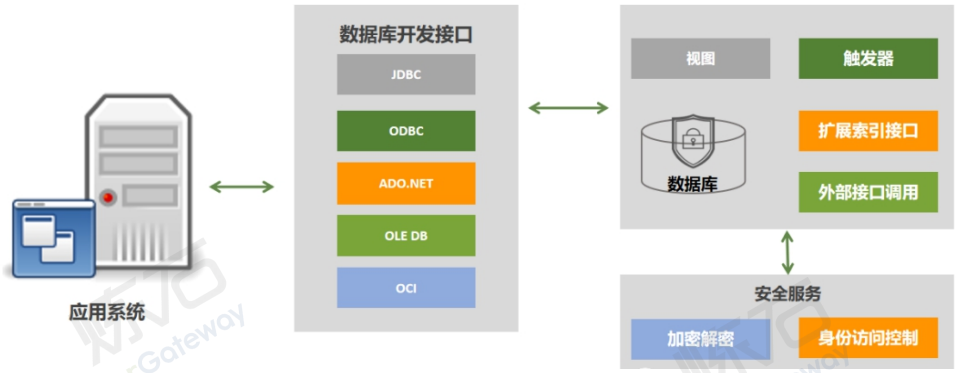


图 7：数据库外挂加密技术原理

### 2）应用场景

如果查询涉及的加密列不多，查询结果集中，且包含的数据记录也相对不多时，可以考虑使用数据库外挂加密技术对数据库进行加密。

### 3）优势

**1、独立权控体系。**使用数据库外挂加密技术，可以在外置的安全服务中提供独立于数据库自有权控体系之外的权限控制体系，适用于对“独立权控体系”有相关需求的场景，可以有效防止特权用户（如 DBA）对敏感数据的越权访问。

### 4）挑战

**1、仅支持 Oracle 等少量数据库类型。**数据库外挂加密，目前大多数的技术实现形式，存在功能性缺陷，仅仅支持对 Oracle 等少量数据库的加解密，对于 MySQL、SQL Server 以及国产数据库等难以支持；

**2、数据库性能表现不佳。**数据库外挂加密是通过多级视图及创建于其上的触发器进行外部接口调用来实现加解密，触发器的运行机制要求对加密表中的每一条数据中的每个加密列的读写都会进行一次外部接口调用，因此，当遇到比如“查询中涉及的加密列较多”等情况时，对数据库的整体性有一定影响；

**3、可扩展性差。**在业务变化引起数据库表结构发生变化时，需要对外挂程序进行调整，甚至需重新定制开发，需专业人员维护。

## 技术七：TDE 透明数据加密

### 1）原理解析

**部署位置：**数据库

**原理：**透明数据加密（Transparent Data Encryption，简称为 TDE）指把数据信息即明文转换为不可辨识的形式即密文的过程。数据在落盘时加密，在数据库内存中是密文，一旦拔盘，由于数据库文件无法获得解密密钥而无法打开，从而起到保护数据库中数据的效果。

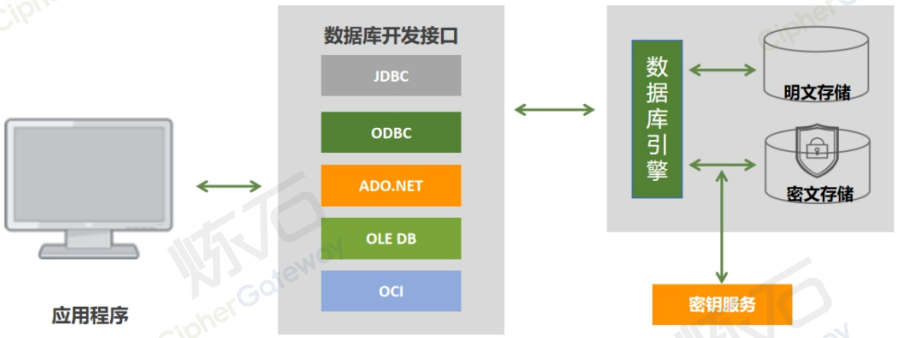


图 8：透明数据加密技术原理

### 2）应用场景

透明数据加密技术适用于对数据库或磁盘中的数据文件执行实时加解密的应用场景，尤其是在对数据加密透明化有要求，以及对数据加密后数据库性能有较高要求的场景中。

### 3）优势

**1、独立权控体系。**与数据库外挂加密形同，使用插件形式的透明数据加密技术，同样可以在外置的安全服务中提供独立于数据库自有权控体系之外的权限控制体系；

**2、性能优势。**透明数据加密技术只对数据库引擎的存储管理层进行了性能增强，不影响数据库引擎的语句解析和优化等处理过程，数据库自身性能得以更好保留，透明数据加密技术在数据库加密技术中，性能上面具有明显优势，对数据库性能有较高要求的场景，可以优先考虑这种加密方式。

### 4）挑战

**1、数据库类型适用性上有限制。**透明数据加密因使用插件技术，对数据库的版本有较强依赖性，且仅能对有限几种类型的数据库实现透明数据加密插件，在数据库类型适用性上有一定限制；

**2、防护能力较弱。**TDE 本身是一种落盘加密技术，数据在内存中处于明文状态，需要结合其他访问控制技术使用。

## 技术八：UDF 用户自定义函数加密

### 1）原理解析

**部署位置：**数据库

**原理：**UDF（User Defined Function）用户自定义函数加密，目的是在已有数据库功能的基础上扩展更丰富的业务诉求，其原理是在数据库支持的形式上，通过定义函数名称及执行过程，实现自定义的处理逻辑。

### 2）应用场景

UDF 用户自定义函数加密，适用于某些数据库不支持国密算法的场景，该加密技术可以实现基于数据库的国密算法数据加解密。

### 3）优势

**1、扩展能力强。**该加密技术适用于对数据有“定制化实现”的场景化需求，能够根据用户的业务需求，对数据实现丰富多样的处理。

### 4）挑战

**1、通用性低。**该加密技术需要根据不同数据库的类型，做相对应的定制化实现。

## 技术九：TFE 透明文件加密

### 1）原理解析

**部署位置：**文件系统

**原理：**透明文件加密（Transparent File Encryption，简称为 TFE），是在操作系统的文件管理子系统上部署加密插件来实现数据加密。在正常使用时，计算机内存中的文件以受保护的明文形式存放，而硬盘上保存的数据是密文，如果没有合法的使用身份、访问权限以及正确的安全通道，加密文件都将以密文状态保护。

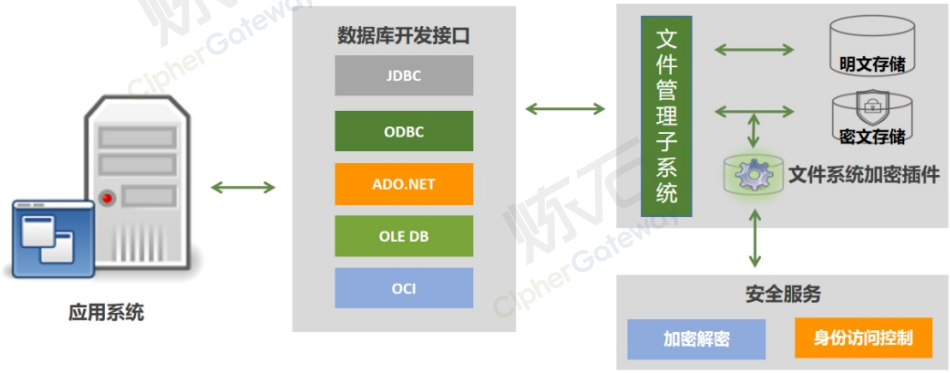


图 9：透明文件加密技术原理

### 2）应用场景

透明文件加密技术几乎可以适用于任何基于文件系统的数据库存储加密需求，尤其是原生不支持透明数据加密的数据库系统。但是，由于文件系统加密技术无法提供针对数据库用户的增强权限控制，因此对于需要防范内部数据库超级用户的场景并不适用。

### 3）优势

**1、相对的性能优势。**在数据加密的处理性能方面，透明文件加密技术拥有相对的优势。一方面，因为透明文件加密技术与数据库的无关性，因此该技术不会对数据库引擎处理和处理数据的逻辑有任何影响；另外一方面，透明文件加密技术因为是在操作系统的文件管理子系统上部署加密插件来实现数据的加密功能，因此会增加数据库系统和磁盘存储进行交互时的工作量，从而对数据库系统整体性能造成部分损失。总体来看，透明文件加密技术拥有相对的性能优势；

**2、可与应用进程绑定。**透明文件加密可以适用于对应用进程有绑定需求的场景，只有授权的应用访问文件时，才能获得明文，非授权应用，只能获取密文。

### 4）挑战

**1、管理员风险。**由于文件系统加密技术的数据库无关性，因此，该加密技术不具备对系统用户增强的权限控制能力，无法防止内部人员包括系统管理员和数据库 DBA 对加密数据的访问。

## 技术十：FDE 全磁盘加密

### 1）原理解析

**部署位置：**存储硬件

**原理：**全磁盘加密（Full Disk Encryption，简称 FDE）是指通过动态加解密技术，对磁盘（硬盘）或分区进行动态加解密的技术。FDE 的动态加解密算法位于操作系统底层，其所有磁盘操作均通过 FDE 进行：当系统向磁盘上写

入数据时，FDE 首先加密要写入的数据，然后再写入磁盘；反之，当系统读取磁盘数据时，FDE 会自动将读取到的数据进行解密，然后再提交给操作系统。

### 2）应用场景

全磁盘加密技术适用于磁盘（硬盘）上所有数据（包括操作系统）进行动态加解密的场景，但由于不能提供针对用户的增强权限控制，无法满足对内部超级用户泄露敏感数据的风险防范需求。

### 3）优势

**1、优秀的性能优势。**磁盘加密技术通过存储设备自身的物理结构实现，能够最大化发挥存储设备本身的硬件能力，能够对上层数据库系统提供无损的性能服务；**2、部署、实施简单。**磁盘加密仅需对进入磁盘的数据进行加密，部署、实施均较为简单高效。

### 4）挑战

**1、数据泄露风险。**该加密技术因为缺少访问控制能力，因此，一旦磁盘挂载口令泄露，就有数据泄露的风险。

| 加密技术 | 部署位置 | 加密粒度 | 性能 | 防 DBA | 数据库复杂计算 | 实施成本 |
| --- | --- | --- | --- | --- | --- | --- |
| DLP 终端加密 | 终端 | 文件 | 中 | / | / | 中 |
| CASB 代理网关 | 终端-应用服务器间 | 文件/字段 | 较高 | 支持 | 影响 | 较高 |
| 应用内加密（集成密码 SDK） | 应用服务器 | 文件/字段 | 高 | 支持 | 影响 | 高 |
| 应用内加密（AOE 面向切面） | 应用服务器 | 文件/字段 | 高 | 支持 | 影响 | 低 |
| 数据库加密网关 | 应用服务器-数据库间 | 字段 | 较高 | 支持 | 影响 | 较高 |
| 数据库外挂加密 | 数据库 | 字段 | 低 | 不支持 | 不影响 | 较高 |
| TDE 透明数据加密 | 数据库 | 字段/表空间 | 高 | 不支持 | 不影响 | 低 |
| UDF 用户自定义函数加密 | 数据库 | 字段 | 中 | 不支持 | 不影响 | 低 |
| TFE 透明文件加密 | 文件系统 | 文件 | 中 | 不支持 | 不影响 | 中 |
| FDE 全磁盘加密 | 存储硬件 | 磁盘/卷 | 高 | 不支持 | 不影响 | 低 |

综上所述，十种数据存储加密技术在应用场景以及优势挑战方面各有侧重点，DLP 终端加密技术、CASB 代理网关侧重于企业 PC 端的数据安全防护；应用内加密（集成密码 SDK）、应用内加密（AOE 面向切面加密）侧重于企业应用服务器端的数据安全防护；数据库加密网关、数据库外挂加密、TDE 透明数据加密、UDF 用户自定义函数加密则侧重于数据库端的数据安全防护；TFE 透明文件加密、FDE 全磁盘加密则分别侧重于文件系统、磁盘的数据安全防护。

时代和科技正以前所未有的速度发展，数据安全建设的工作势在必行，在了解数据安全防护的必要性和迫切性的前提下，具体分析相关的数据存储加密技术原理，探究数据加密技术具体运用，总结不同形式的数据存储加密技术，提出更合理、更安全的数据防护措施，这对数据安全防护的建设工作有着积极影响，能够全面保障数据的安全性，助力我国数字化建设进程的健康发展。**作为数据安全创新公司，炼石也将不断探索技术创新思路，提高数据存储加密技术的适用性，为网络信息行业健康发展助力。**

# 公司介绍

数据实战化加密 安全新合规平台

炼石网络是一家基于密码与系统安全技术的数据安全创新公司，提倡“以数据为中心的新安全理念”，自主研发了 CASB 业务数据安全平台和高性能国密产品，开创性的实现免开发改造应用、敏捷实施细粒度数据保护，该产品入选工信部 2020 年网络安全技术应用试点示范推荐项目，并夺得第七届互联网安全大会(ISC 2019)首届“创新独角兽沙盒大赛”总冠军。基于 AOE 面向切面数据安全技术，将安全与业务在技术上解耦、但又在能力上融合交织 ，实现主体到应用内用户、客体到字段级的防护，打造“以密码技术为核心，访问控制、审计等多种安全技术互相融合”的实战化数据安全防护体系。炼石为政府、金融、教育医疗文旅、工业央企商业等行业用户，提供个人信息保护、商业秘密保护以及国密合规改造方案，让数据共享更安全、更有价值。

# 让数据共享更安全、 更有价值

北京炼石网络技术有限公司
BEIJING LIANSHI NETWORKS TECHNOLOGY CO.,LTD.

010-88459460

北京市海淀区北三环西路32号恒润国际大厦

sales@ciphergateway.com