

数据存储加密技术白皮书

V2.0

2026 年 10 月

北京炼石网络技术有限公司

Beijing Lianshi Networks Technology Co., Ltd.

目 录

前 言	1
以合规立基线，以实战验效果	3
数据流动中的安全控制点	6
十种数据存储加密技术特性分析	9
技术一：DLP 终端加密技术	9
技术二：CASB 代理网关技术	10
技术三：应用内加密技术（集成密码 SDK）	12
技术四：应用内加密技术（AOE 面向切面加密）	14
技术五：数据库加密网关技术	16
技术六：数据库外挂加密技术（FGDE 细粒度动态加密）	18
技术七：TDE 透明数据加密技术	21
技术八：UDF 用户自定义函数加密技术	23
技术九：TFE 透明文件加密技术	25
技术十：FDE 全磁盘加密技术	27
存储加密技术的选型路径	33
附录 数据存储加密的另外五个分析维度	34
结 语	37
公司介绍	38

前言

进入“十五五”时期，数据作为新型生产要素，伴随大模型、智能体等人工智能技术加速应用，在跨场景复用和持续迭代中释放出更强的乘数效应。数据价值加快释放，安全风险伴生演进。数据流动范围扩大，治理边界随之延伸；多源数据集中汇聚，使单点失守更容易演变为批量泄露和链式影响。面对时代新形势，国家持续健全数据安全制度体系，修正后的《网络安全法》自 2026 年 1 月 1 日起施行，与《密码法》《数据安全法》《个人信息保护法》共同构成数据安全的制度基础，数据安全要求由原则性“应当保护”转向刚性约束。

制度要求最终要落到数据处理的具体环节。在数据全生命周期中，存储是价值沉淀与风险累积的交汇点，分散产生的数据在此汇聚，规模、敏感程度和关联价值不断叠加，集中面临数据窃取、泄露、滥用等风险。也正因如此，商用密码应用安全性评估（以下简称密评）的判定体系将第三级及以上信息系统“未采用密码技术保证重要数据在存储过程中的机密性”列为无缓解措施的高风险项。而密码技术可以直接作用于数据本身，在边界防护和访问控制失效时仍能发挥保底作用，是解决存储安全问题兼具经济性与可靠性的基础手段。这是本白皮书聚焦数据存储加密的原因。

存储并不是数据流转路径上的一个孤立节点。在典型的信息系统中，数据自终端产生，经应用服务器处理，写入数据库或文件系统，最终落在磁盘与存储层，其间还会以缓存、日志、备份、导出文件等形态多次落盘。加密可以施加在这条路径上的任何一个环节，但施加的位置不同，明文暴露的范围、密钥的归属、对业务的影响和在密评中的判定结论也随之不同。传统按“磁盘、文件、数据库”等介质分类的视角看不到这些差别，因此有必要沿数据流转路径、以安全控制点为线索来分析存储加密技术，并在讨论每一种技术时围绕三个问题展开：加密实施在哪一个控制点，明文在哪些环节仍然存在，密钥由谁掌握、按什么规则释放。这三个问题

的答案，影响了一种技术能防住什么、防不住什么，也影响了它在合规评价中的确定性。

循着这一思路，本白皮书沿典型信息系统的数据流转路径，选取十种具有代表性的存储加密技术进行分析。由于 2026 年 3 月中国密码学会密评联委会更新发布《商用密码应用安全性评估 FAQ》（第四版，以下简称 FAQ 第四版），以应用是否对数据资源本身加密为依据，对应用和数据安全层面的存储机密性给出分情形的裁量标准，使不同加密路线在密评中的结论有了明确区分。因此，与 2022 版相比，本次修订以 FAQ 第四版作为合规判定的统一尺度，着重从加密位置、明文暴露边界、密钥掌握方和实际防护效果等方面展开比较，并把“加密后明文还在哪里”“密钥在谁手里”这两个最影响实际防护效果的问题显性化；同时补充各技术的演进方向，以附录的五个分析维度回应密文可计算、后量子迁移等新问题，力求为不同场景下的技术选型给出可操作的判断参考。

数据存储加密的价值，不在于系统中“出现了密文”，而在于围绕数据建立一套可验证、可持续的保护机制。希望本白皮书能帮助从事数据安全规划、密码应用建设和密评准备工作的技术与管理人员快速了解数据存储加密技术的全貌，并为其在场景适用性判断、相关技术与产品选型等方面提供参考。

以合规立基线，以实战验效果

存储安全不能只关注数据“能否保存”，更要回答数据能否以受保护、未授权难利用、可管控、可追溯的状态持续留存。围绕这一目标，业务上每一种“希望数据发生什么”的需求，都伴随相应的“不希望发生什么”的风险。希望数据集中以便分析，就要防集中后的批量泄露；希望数据被应用便捷读取，就要防应用被越权利用；希望数据长期留存，就要防留存期间介质失控与密钥失效。风险内生于处理活动，安全措施就必须落到具体的系统、数据对象、访问主体和操作行为上，而不能停留在“已经加密”的笼统表述。

衡量存储安全是否做到位，需要以合规立基线、以实战验效果。炼石认为，密码应用合规可分为过程合规与结果合规：前者关注密码算法、密码产品、密钥管理、部署配置和运行管理是否符合要求，后者关注数据机密性、完整性、真实性等安全目标是否达到。实战验证则以应对实际风险的安全效果为牵引，检验各项措施在具体威胁场景下是否真正有效。合规形成可执行、可重复验证、可审计的安全基线，实战回答“防没防住”，二者相互支撑而不能相互替代。而合规基线能否成立，取决于由谁验证、如何验证。

密码技术应用是否正确、合规、有效，要通过权威、法定的评测机制加以验证。密评是国家法定的合规检验活动，对信息系统密码应用的合规性、正确性和有效性作出权威评价，其结论是相关系统建设验收和运行阶段合规检查的重要依据。密评依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》和中国密码学会密评联委会（以下简称密评联委会）《商用密码应用安全性评估量化评估规则（2023 版）》，采用打分制，满分 100 分、覆盖 8 个方面、共 41 个测评单元，通过要求为不低于 60 分（含 60 分）且无高风险项。在密评的判定体系中，对第三级及以上信息系统，“未采用密码技术保证重要数据在存储过程中的机密性”被明确列为高风险项，且无缓解措施可用。这意味着对第三级及以上信息系

统，重要数据存储机密性不满足要求且无缓解措施时，评估结论即为“不符合”，不能依靠其他测评单元的得分弥补。从炼石承接密改项目的实践看，应用和数据安全层面与密码应用直接相关的测评单元合计约 21 分，是密评失分最集中、也最依赖技术改造才能解决的部分。同时，《商用密码应用安全性评估管理办法》第九条要求，重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估（实践中主要包括关键信息基础设施、网络安全等级保护第三级及以上系统、政务信息系统等）。密评由此成为存储加密从“建议动作”转为“限期动作”的直接驱动力。

然而，在密评密改建设中，同样是“数据库里有密文”，磁盘加密、数据库透明加密与应用对数据本身加密，在加密实施层次、明文暴露范围和访问控制机制上差异很大，此前缺乏统一的判定尺度，密评实践中往往难以区分。2026 年 3 月，密评联委会更新发布 FAQ 第四版，进一步明确了应用和数据安全层面存储机密性的判定依据，并针对不同加密实现路径给出分情形的有效性裁量标准。

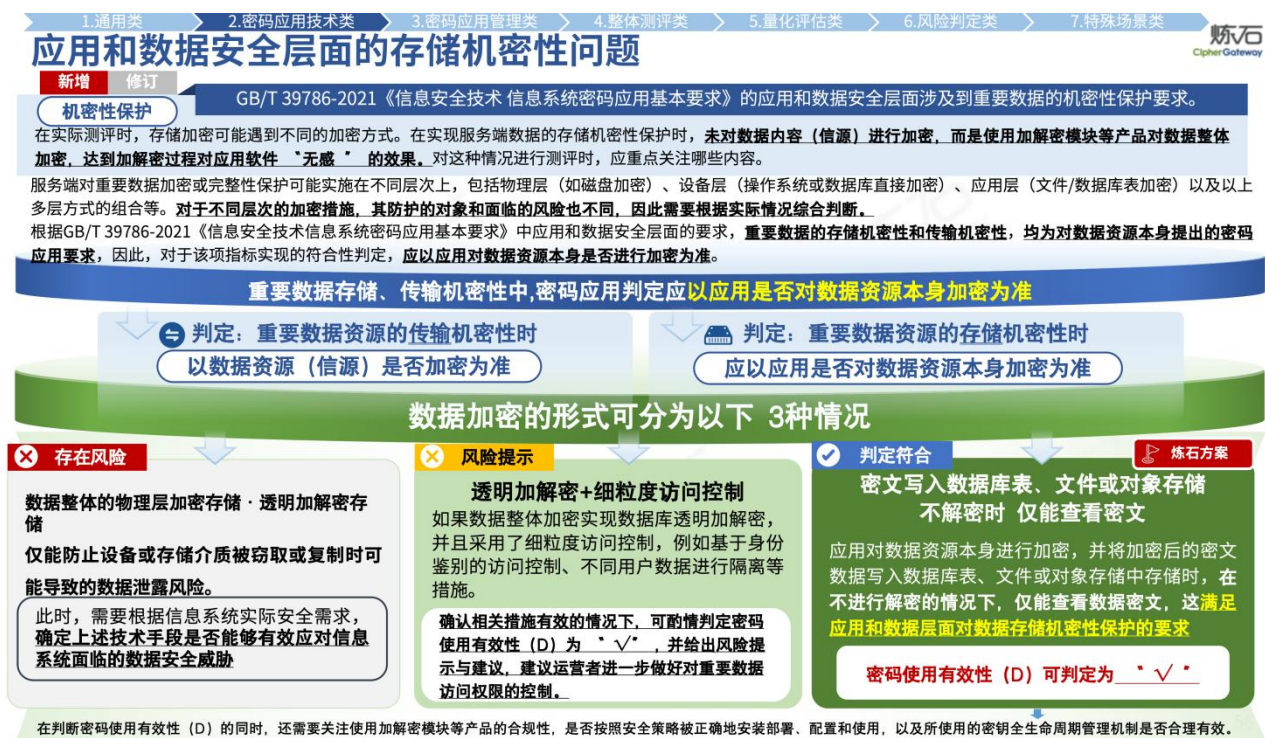


图 1《商用密码应用安全性评估 FAQ》（第四版）应用和数据安全层面的存储机密性问题图解

如图 1 所示，FAQ 第四版第 23 条“应用和数据安全层面的存储机密性问题”明确，重要数据的存储机密性应以应用是否对数据资源本身加密为准，并将数据加密的形式分为以下三种情况：其一，对于数据整体的物理层加密存储，仅能防止设备或存储介质被窃取或复制时可能导致的数据泄露风险，此时需要根据信息系统实际安全需求，确定上述技术手段是否能够有效应对信息系统面临的数据安全威胁；其二，数据整体加密实现数据库透明加解密，并采用了细粒度访问控制（如基于身份鉴别的访问控制、不同用户数据隔离等措施），确认相关措施有效的情况下，可酌情判定密码使用有效性（D）为“√”，并给出相应风险提示与建议；其三，应用对数据资源本身进行加密，并将加密后的密文写入数据库表、文件或对象存储，未解密时仅能查看密文，可直接满足存储机密性保护要求，密码使用有效性（D）可判定为“√”。需要注意的是，应用本身一般无法对所有数据都进行加密保护，只对重要数据进行加密保护。密码使用有效性的判定，还应综合核查所用密码产品的合规性，密码技术部署、配置和使用的正确性，以及密钥全生命周期管理机制的有效性。据此，第（1）种情况对应物理层加密存储，第（2）种情况在数据库透明加解密的基础上以是否配套细粒度访问控制为判定条件；第（3）种情况以应用是否对数据资源本身加密、密文是否写入数据库表、文件或对象存储且未解密时仅能查看数据密文为判定要件。

需要把握的是，第（3）种情况明确以应用作为加密实施主体，并非只要密文落地就属于第（3）种情况。第（1）种情况的定义性特征是“数据从外部看始终为明文状态”，因此判断一种实现属于第（3）种还是透明加解密类，关键在于加解密是否在应用进程之内完成、明文是否收敛于应用的授权上下文：凡加解密在应用进程之外完成、应用无差别读取即得明文的实现（如网关侧、外挂侧、数据库侧、文件系统侧透明加解密），无论密文写在哪一层，都应按第（1）、（2）种情况的逻辑评价。同时，第 23 条判定的是加密实施主体、加密对象与配套控制措施，并不评价明文暴露边界与密钥控制权；落入同一情形的技术，其实际防护效果仍存在差异。这正是本白皮书以 FAQ 第四版作为统一合规尺度、逐一标定各类存储加密技术判定确定性的原因。

数据流动中的安全控制点

炼石免改造数据安全：将密码等安全能力投送到真实的数据处理流程中

以往数据保护习惯把加密施加在承载数据的“容器”上——磁盘、文件系统乃至数据库整体，防的是介质被窃取、环境被攻破。但数据在业务系统中并非静止于某一介质，而是沿终端、应用、数据库、文件与存储不断流转，明文在流转的每一个环节都可能暴露。因此，数据存储加密的难点，并不只是将数据以密文形式写入某一存储介质，而是要在数据流转过程中选择适当的安全控制点，对需要保护的数据资源本身实施加密，并有效控制明文暴露范围，降低数据被未经授权读取和利用的风险。

本白皮书所讨论的数据，既包括以数据库二维表等形式组织和存储的结构化数据，也包括文档、图片、视音频等不具有固定结构的非结构化数据。传统的“数据库加密”主要面向结构化数据，关注数据写入数据库后的密文存储状态；但即便是结构化数据，也要经过应用处理、数据库读写、文件生成、对象存储、备份归档等多个环节，数据库只是数据流转和存储的控制点之一。因此，“数据库存储加密”只是“数据存储加密”的子集，判断一种存储加密技术是否有效，不能只看存储介质或者数据库文件中是否存在密文，还应结合加密的实施层次、实际保护对象、明文暴露边界以及配套访问控制措施综合分析。

基于此，本白皮书以“数据”为中心，沿典型 B/S 三层信息系统架构的数据流转路径，在终端、应用服务器、应用与数据库之间、数据库、文件系统和存储层等数据业务处理点上，结合业内常见实现，选取十种具有代表性的存储加密技术逐一分析，总体分布如图 2 所示。每一种技术均从实现原理、应用场景、优势、挑战与技术演进五个方面展开分析，并以加密控制点（部署位置）、加密粒度、明文暴露边界、密钥掌握方、性能、防范 DBA、数据库复杂计

算、实施成本以及第 23 条对应情形等维度进行横向对比。在正文的控制点维度之外，附录补充密钥信任边界、密文可计算性、密文形态、保护对象与算法生命周期五个分析维度，供方案设计与技术选型时交叉参照。



注：控制点、明文暴露边界与密钥掌握方对应表1；数据库列中⑥FGDE的明文暴露边界为数据库进程及授权主体侧，密钥由外部密钥管理系统掌握。分档依据《商用密码应用安全性评估FAQ》（第四版）第23条：第（1）种为数据整体的物理层加密存储，仅能防止设备或存储介质被窃取或复制导致的泄露，需按信息系统实际安全需求判断其有效性；数据库透明加解密配套细粒度访问控制的为第（2）种，可酌情判定密码使用有效性（D）为符合并给出风险提示；第（3）种为应用对数据资源本身加密并将密文写入数据库表、文件或对象存储，（D）可判定为符合。加解密在应用进程之外完成的，无论密文写在哪一层，均按第（1）、（2）种评价。第23条判定的是加密实施主体、加密对象与配套控制措施，不评价明文暴露边界与密钥控制权——落入同一档的技术，实际防护效果仍有差异。最终判定以测评机构结论为准。

图 2 数据存储加密技术总览图

承接前述 FAQ 第四版的裁量标准，在图 2 所列技术中，由应用对数据资源本身加密并将密文写入数据库表、文件或对象存储的实现方式，具有更明确的合规判定依据；落入同一判定情形并不意味着防护效果相同，明文暴露边界与密钥掌握方仍需结合表 1 分别评价。实现应用对数据资源本身加密的路径，从实施方式看主要有两类：一是由应用调用外部密码机等密码硬件对数据本身完成加密；二是采用应用层免改造加密技术（如炼石 AOE 面向切面加密方案）。

前者虽能实现“对数据资源本身加密”，但仍需应用开发改造以完成密码接口调用，实施周期长、改造成本高；后者通过面向切面技术，在不修改应用代码的前提下自动拦截数据流并完成加密，将密文写入数据库表、文件或对象存储，实施敏捷、维护成本低。相较于数据库侧透明加密，炼石应用层免改造加密方案在密评合规确定性上更具优势；相较于依赖应用开发改造调用密码接口的方式，则在实施敏捷性上更具优势。

炼石认为，在实际应用中，要结合用户场景和适用性需求，选择一种或组合多种存储加密技术，优势互补，打造“以密码技术为核心，访问控制、审计等多种安全技术相互融合”的密码安全一体化防护体系，将密码等安全能力投送到真实的数据处理流程中，既满足合规基线要求，也经得起实战检验。

十种数据存储加密技术特性分析

技术一：DLP 终端加密技术

1、原理解析

- 部署位置：终端
- 原理：DLP（Data Loss Prevention，数据泄露防护）终端加密技术，目的是管理企业终端上（主要是 PC 端）的敏感数据。业界经典 DLP 以敏感内容识别与阻断为核心，本白皮书所述“DLP 终端加密”特指国内终端安全产品中与 DLP 策略联动的文档透明加密能力，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，加密密钥由管理平台统一生成和下发，并结合企业的数据管理要求和分级分类策略，对下载到终端的敏感数据进行加密，从而将加密应用到企业数据的日常流转和存储中。文件被授权程序读入内存时自动解密，未经授权复制出管控范围的文件保持密文；截屏、打印等旁路通道仍需结合外发管控策略，主要适用于非结构化数据的保护。



加密与使用权限随文件在终端流转过程中保持，未经授权复制到管控范围外仅为密文

图 3 DLP 终端加密技术原理

2、应用场景

DLP 终端加密技术主要适用于企业终端数据的安全管理，在原有安全防护能力之上，可降低以下场景的数据泄露风险：

- (1) 操作失误或无意识外发导致重要数据泄露；
- (2) 通过打印、剪切、复制、粘贴、另存为或外设拷贝等操作造成数据泄露；
- (3) 离职人员通过 U 盘、移动硬盘等方式私自拷贝带离机密资料；
- (4) 移动笔记本被盗、丢失或维修等造成数据泄露。

3、优势

文件外发强管控。和其他终端安全技术相比，能够强制实现重要敏感文件的外发管控，从而实现对数据的“事前防护”，可防范一定程度的“有意泄露”。

4、挑战

终端适配困难、运维成本较高。企业终端一般具有操作系统众多、终端类型复杂、文档使用场景多样等特点，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。在移动终端，由于存在权限问题，技术落地难度大。密评定位：DLP 终端加密对终端文件实施透明加解密，文件被授权程序读入内存时自动解密，属于 FAQ 第四版第 23 条所述数据整体加密实现的透明加解密，其判定同样取决于是否配套细粒度访问控制；此外，受保护对象是否属于信息系统的重要数据，需结合系统定级与数据识别结果判断。

5、技术演进

终端文件加密正在与数据分类标签、持续权限控制和云协同结合，使加密及使用权限随文件流转保持，防护范围从本地终端延伸至云端协作。但此类能力通常依赖特定办公生态和身份体系，跨平台、跨组织协同仍需验证。

技术二：CASB 代理网关技术

1、原理解析

- **部署位置：**用户/终端-云服务之间

- **原理：**CASB 代理网关（Cloud Access Security Broker，云访问安全代理）是一种委托式安全代理技术，将网关部署在目标应用的客户端和服务端之间，无需修改应用代码，但需针对目标应用做协议与语义适配。网关对客户端请求进行解析，识别其中包含的敏感数据，结合用户身份和安全策略实施脱敏、拦截等管控措施，可同时管控结构化数据和非结构化数据。部分 CASB 产品在采用加密、令牌化等处理模式时，还可在数据进入云服务前完成敏感字段保护。

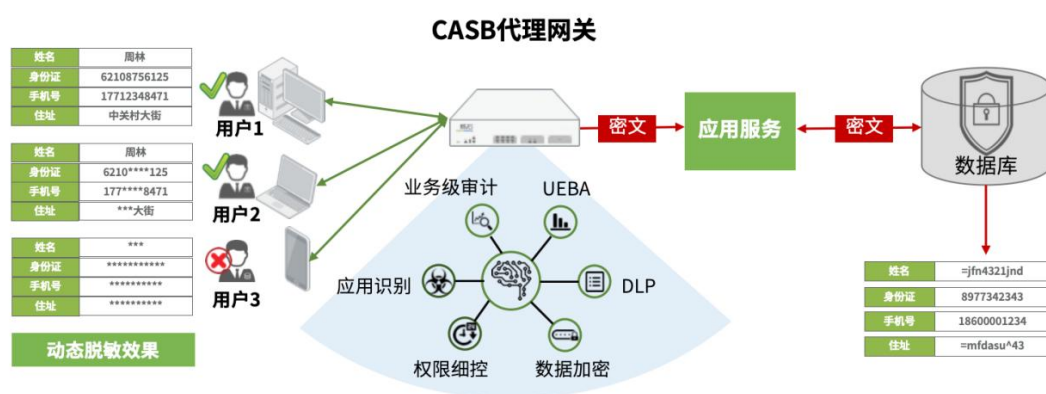


图 4 CASB 代理网关技术原理

2、应用场景

企业大量业务系统托管在云服务商处，HR、社保、报销、OA 等事务普遍采用 SaaS 服务；企业想要享受便捷的云服务，又不想失去对自身数据的控制权，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：能识别用户访问云资源时使用的是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

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，该位置可以获取到丰富的业务上下文，可以基于用户、资源、操作和业务属性，灵活利用访问者所对应属性集合影响是否有权访问目标数据，如部门、区域、职位、动作、目标数据类型、时间等，从而在复杂业务场景下实现对数据的安全防护。

4、挑战

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，适配工作量取决于目标应用的数量和复杂度以及安全管控粒度。密评定位：CASB 代理网关是否形成存储密文取决于具体产品及配置：仅实施脱敏、拦截等管控而未对数据本身加密时，不构成存储机密性的符合性证据；在采用加密或令牌化对数据资源本身处理并将密文写入云服务存储的模式下，加密由网关而非应用实施，应按第 23 条第（1）、（2）种情况的逻辑评价，其明文暴露边界包含网关及用户侧，密钥由网关侧掌握。需要注意的是，该模式对用户侧应用同样透明，用户经授权访问时即得明文，网关基于用户身份与安全策略的管控被确认有效时，可对应第（2）种情况。

5、技术演进

CASB 由单一代理形态向 API 连接、反向代理和浏览器内控制等组合形态发展，可同时覆盖静态文件扫描和实时会话控制。该演进增强了云应用可见性与策略执行能力，但其本质仍是云访问控制和数据防泄漏能力，是否形成存储密文取决于具体产品及配置。

技术三：应用内加密技术（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）指应用系统通过开发改造的方式，与封装了加密业务逻辑的密码 SDK 进行集成，并调用其加解密接口，使目标应用系统具备数据加密防护能力。

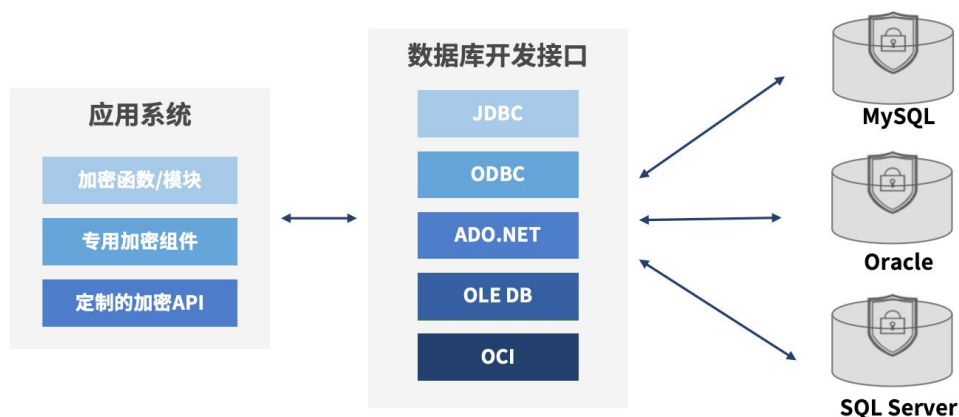


图 5 应用内加密（集成密码 SDK）技术原理

2、应用场景

通常情况下，当应用系统仅对数量有限的敏感数据存在加密需求时，适合采用应用内加密（集成密码 SDK）技术，主要场景包括：需要加密处理的敏感数据代码逻辑在业务系统中分布不多，或者需要加密处理的敏感数据对应的表或字段相对较少。

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绝大多数问题，不依赖特定数据库的原生加密能力；

（2）灵活性高。应用服务端加密可与业务逻辑紧密结合，开发人员能够在应用开发过程中按业务需要，对相关业务中的敏感数据灵活实施加密处理，所使用的加密函数、加密密钥等也均可根据业务逻辑需求自行选择。

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成本，时间周期较长，后期实施和维护成本较高，也面临大量代码改造带来的潜在业务风险；

（2）对应用开发人员要求高。对业务开发人员来说，正确合规使用密码技术具有一定门槛。比如在实际应用中，会出现应用开发人员密钥使用不合规或安全风险等情况。

（3）密评定位：符合第 23 条第（3）种情况。应用内加密（集成密码 SDK）通过调用密码接口对数据资源本身完成加密，并将密文写入数据库表、文件或对象存储，未解密时仅能

查看数据密文，符合 FAQ 第四版第 23 条第（3）种情况，密码使用有效性（D）可判定为符合。

5、技术演进

应用加密 SDK 逐步采用信封加密、数据密钥与主密钥分层、密钥管理系统（KMS）/硬件安全模块（HSM）托管及多密钥封装等机制，可改善大规模应用中的密钥隔离和轮换管理；但应用代码改造、密码接口合规使用及长期维护成本并未消失。

技术四：应用内加密技术（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，能以免开发改造方式，实现应用系统中结构化数据和非结构化数据的存储加密，并提供细粒度访问控制、丰富脱敏策略以及数据访问审计功能，为应用打造较为全面、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，在应用运行时拦截数据访问调用（如 JDBC 层 SQL 执行），完成加密后写入数据库。对于文件和对象存储，可在相应存储接口或数据流控制点完成加密后写入。

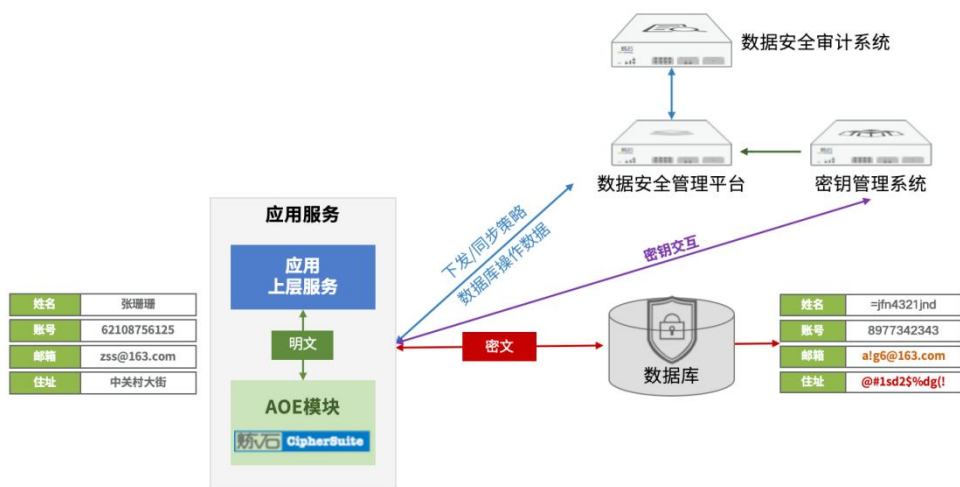


图 6 应用内加密（AOE 面向切面加密）技术原理

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改造的、可敏捷实施的高性能数据安全防护。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，灵活性高，并支持分布式部署、集中式管控，既可对单个应用实施防护，也可对上百个应用批量防护。

3、优势

（1）**数据加密与业务逻辑解耦。**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；

（2）**不影响业务运营。**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，能够实现以配置的方式敏捷部署实施，不中断业务运行，无需停机改造，也不需要变更既有的数据访问逻辑；

（3）**基于细粒度权限控制的数据安全防护。**该加密技术可针对应用打造“主体到人、客体到字段”的安全防护体系，能够根据不同属性的人群，实施细粒度的权限控制，实现对企业内部人员的敏感数据访问最小化授权。

4、挑战

（1）AOE 需要适配不同的编程语言和应用框架。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。此外，加密字段对数据库侧模糊检索、排序、聚合等运算存在影响，需结合密文索引等机制处理，其中支持等值检索的密文索引若采用确定性机制，同样需评估数据分布泄露风险；存量数据需完成初始化加密。

（2）密评定位：符合第 23 条第（3）种情况。应用内加密（AOE 面向切面加密）技术及应用进程之内对数据资源本身完成加密，并将密文写入数据库表、文件或对象存储，未解密时仅能查看数据密文，符合 FAQ 第四版第 23 条第（3）种情况，密码使用有效性（D）可判定为符合。相较于数据整体加密实现的透明加解密（其判定取决于是否配套细粒度访问控制），

该方式的判定不依附于系统另行具备的访问控制措施；同时其明文暴露边界收敛于应用进程的授权上下文，密钥由应用侧或密钥管理系统掌握，在合规判定之外的实际防护效果亦相应不同。

5、技术演进

AOE 正从单应用切面走向统一控制面。保护对象由数据库字段扩展至文件与对象存储，策略、密钥、审计由多应用共用一套治理体系，并向分布式与云原生部署形态适配；持续延伸至向量数据库、向量检索等 AI 数据基础设施，并通过自研拦截器组件拓展复杂异构环境的适配能力。

技术五：数据库加密网关技术

1、原理解析

- **部署位置：**应用服务器-数据库之间
- **原理：**数据库加密网关是部署在应用服务器和数据库服务器之间的代理网关设备，通过解析数据库协议，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。

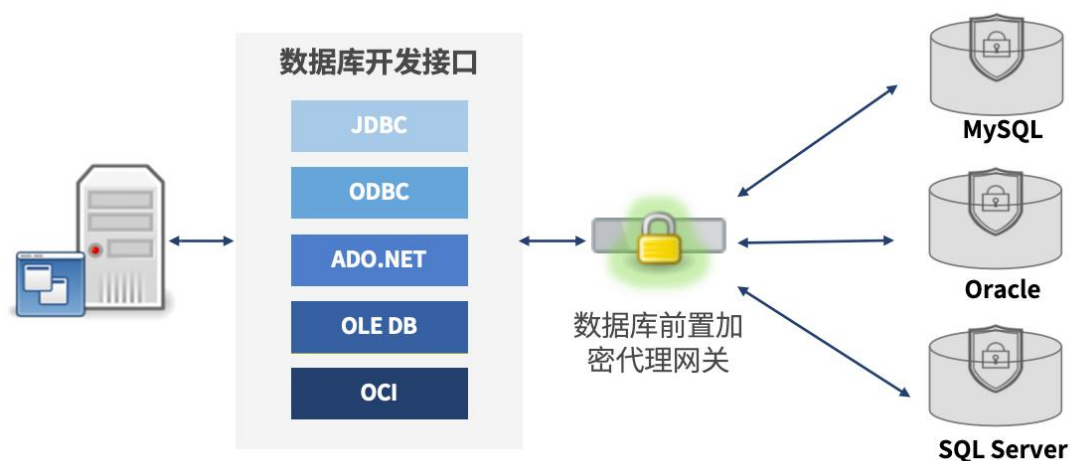


图 7 数据库加密网关技术原理

2、应用场景

数据库加密网关可为数据库提供“入库加密、出库解密”的防护，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，降低数据库文件被直接拖库后泄露明文的风险，并可结合策略识别、拦截高风险 SQL。

3、优势

(1) 应用代码零改造，加解密与业务解耦。相比应用内加密（集成密码 SDK）需要在业务代码中逐处调用密码接口，数据库加密网关以协议代理方式接管加解密，应用代码不作改动、通常仅需调整数据库连接配置，即可获得字段级加密能力，既把开发团队从繁重的密钥处理和加解密逻辑中解放出来，也避免了大量代码改造带来的业务风险；

(2) 具备独立于数据库的权控体系。网关位于应用与数据库之间，可基于数据库账号、来源应用、访问时段和 SQL 特征建立独立的授权与解密策略；密钥由网关侧或外部密钥管理系统掌握，不随数据库一同交付。在密钥独立管理、且不存在绕过网关直连数据库的旁路访问的前提下，可降低数据库管理员（DBA）凭数据库自身权限直接读取敏感明文的风险；

(3) 可与审计、脱敏能力合一部署。由于访问数据库的流量都经过网关，除加密外还可同步实现敏感数据访问审计、动态脱敏和高风险 SQL 拦截，形成一次接入、多种能力叠加的部署形态，减少在数据库前串接多套设备造成的链路复杂度和故障点。

4、挑战

(1) 协议适配与授权合规风险。对于采用私有通信协议的商业数据库，安全厂商开展协议适配时，需要重点关注授权许可、知识产权、版本兼容性及后续升级维护等合规与工程风险；

(2) 高性能和高可用实现难度大。数据库加密网关增加了额外的处理节点，在大数据量和高并发访问场景下，要实现高性能、高可用，面临工程化实现挑战；

(3) 存在库内访问盲区。存储过程、触发器、数据库作业等在数据库内部产生的数据读写不经过网关，无法被加密策略覆盖。

(4) 密评定位：按第（1）、（2）种情况的逻辑评价。数据库加密网关对数据资源本身完成加密并将密文写入数据库表，未解密时仅能查看数据密文，但加密由网关而非应用实施，不满足 FAQ 第四版第 23 条第（3）种情况“应用对数据资源本身进行加密”的要件；网关对应用完全透明，应用侧读取时自动解密，数据对应用而言始终呈明文状态，这一特性与第（1）、（2）种情况所述透明加解密一致，其归属取决于网关侧独立于数据库的授权与解密策略是否被认定为有效的细粒度访问控制。此外，加解密在网关侧完成，明文在网关及上层应用中存在，密钥由网关侧或外部密钥管理系统掌握；存储过程、触发器等库内操作不经过网关，相关数据的加密覆盖情况需另行说明。

5、技术演进

数据库加密网关正与数据库审计、动态脱敏、SQL 风险识别与拦截等能力合并，向统一的数据库安全代理形态发展，并出现安全厂商依托云环境以镜像、托管部署等形态交付的实现。这一演进提高功能集中度和运维便利性，但网关作为数据通路上的独立节点，其性能瓶颈、高可用负担以及对各类数据库协议和版本的持续适配要求并未改变。

技术六：数据库外挂加密技术（FGDE 细粒度动态加密）

1、原理解析

- 部署位置：数据库（库内插件）
- 原理：数据库外挂加密的传统形态，是针对数据库定制开发外挂进程，使进入数据库的明文先经外挂程序加密，形成密文后再插入数据库表中。这种技术使用“触发器”+“多层视图”+“扩展索引”+“外部调用”的方式实现数据加密，在表结构和访问方式保持稳定的前提下，可做到对应用基本透明。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。视图可对表内数据进行过滤、投影、聚集、关联和函数运算，并在视图内调用敏感列解密函数完成数据解密。其新一代形态为 FGDE 细粒度动态加密（Fine-Grained Dynamic Encryption）：借助数据库官方扩展机制在数据库进程内植入

模块，不再改写写入路径，而是在结果集交付环节按访问主体动态判定数据形态（详见本节“技术演进”）。

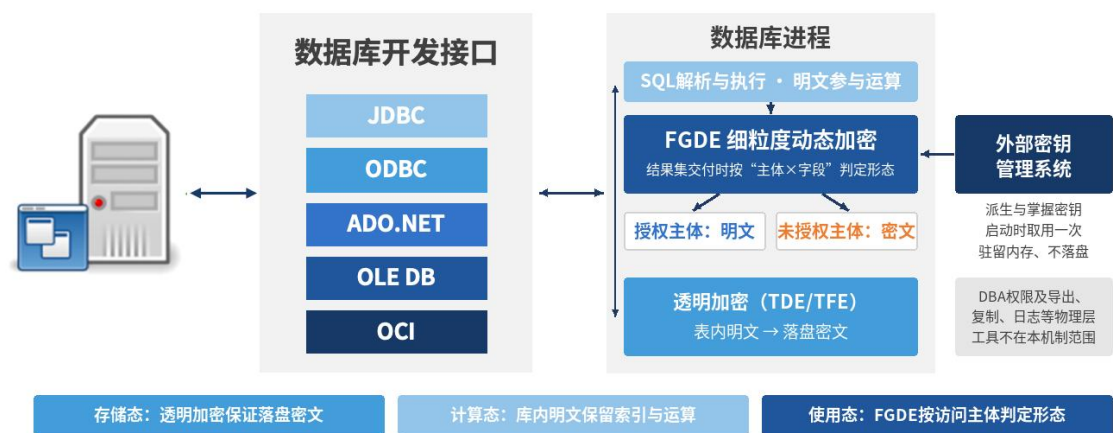


图 8 数据库外挂加密（FGDE 细粒度动态加密）技术原理

2、应用场景

适用于应用侧改造不可行或成本过高的存量系统与第三方套装软件：在已部署透明加密解决落盘密文的基础上，需进一步区分数据库内部访问主体、对未授权账号收敛明文暴露，以满足密评对“细粒度访问控制”的要求；亦适用于对模糊检索、排序、聚合等库内运算有硬性要求、不能接受密文入库的场景。

3、优势

（1）应用免改造、数据库免换。以数据库官方扩展机制装载，不改应用代码、不改表结构与 SQL、不替换数据库二进制；授权主体访问路径全程直通，无额外开销与感知。

（2）细粒度到“主体×字段”的动态判定。主体到数据库用户、客体到字段，加密决策在运行时依访问主体作出，未授权主体经正常 SQL 路径仅能取得密文，是 FAQ 第四版第 23 条第（2）种情况所要求的细粒度访问控制的直接实现。

（3）库内运算能力完整保留。数据在数据库进程内保持明文参与索引、关联与聚合，不存在密文可计算性问题，这是应用侧入库前加密难以兼顾的。

（4）密钥独立管理。密钥由外部密钥管理系统派生与掌握，数据库启动时向密钥管理系统取用一次并驻留进程内存，密钥本身不落盘。

4、挑战

(1) 需逐库适配植入点。各数据库开放的扩展机制不同（协议层插件、视图与自定义函数、钩子等），植入点需按数据库产品逐一验证与维护；

(2) 防护边界限于数据库访问路径。DBA 权限及导出、复制、日志等绕过数据库访问路径的物理层工具不在本机制防护范围内，需与透明加密、权限分离与审计配合；

(3) 不改变存储态。数据在表内仍为明文形态，存储态机密性依赖配合使用的透明加密，单独部署不构成存储机密性的符合性证据；

(4) 密评定位：对应第（2）种情况。FGDE 与透明加密（TFE/TDE）配合使用：存储态由透明加密保证落盘密文，计算态在数据库进程内保持明文以保留索引与运算能力，使用态由 FGDE 在结果集交付环节按访问主体判定形态，未授权主体经应用访问路径只能取得密文。加密由数据库侧插件而非应用实施，数据对授权应用透明，按 FAQ 第四版第 23 条属“数据整体加密实现透明加解密并采用细粒度访问控制”的第（2）种情况，确认措施有效时可酌情判定密码使用有效性（D）为符合并给出风险提示。与 TDE、TFE 的判定依附于系统另行具备的访问控制不同，FGDE 本身即是基于数据库用户身份鉴别的细粒度访问控制措施，判定要件由方案自身闭合。需说明的是，DBA 及绕过数据库访问路径的物理层工具属另行管控范围，明文暴露边界为数据库进程及获授权主体侧，密钥由外部密钥管理系统掌握。

5、技术演进

数据库外挂加密正从“写入路径改写数据”的传统外挂，演进为“读取路径按主体判定形态”的库内细粒度动态加密。前者依赖触发器与多层视图，性能与维护成本随加密列增多而上升；后者依托数据库自身逐步开放的插件、扩展函数与外部密钥管理接口，将加密决策后移到结果集交付环节，并与透明加密分工——透明加密负责存储态，细粒度动态加密负责使用态，计算态保持明文以维持数据库完整运算能力。这使数据库侧路线在不改造应用的前提下也获得第 23 条第（2）种情况的判定路径，成为应用侧加密之外面向存量系统的互补选择。

技术七：TDE 透明数据加密技术

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 TDE）是在数据库内部实现数据落盘加密、读取解密的技术。数据在写入磁盘前由数据库存储引擎完成加密，读取到数据库内存后解密为明文，供已获授权的用户或应用按原有方式处理，应用无需感知加解密过程。当磁盘、数据库文件或备份文件被窃取、脱机复制时，攻击者无法获得相应密钥，只能得到密文，从而降低静态数据被直接读取和利用的风险。Oracle、SQL Server、MySQL 等主流数据库以及国产数据库提供了 TDE 或类似的静态数据加密能力，但支持范围、授权方式和加密粒度因产品与版本而异：多数实现以表空间或整库为单位加密，Oracle 等产品另提供列级加密选项。TDE 并非开箱即用，需要显式配置并完成密钥体系初始化后才会生效。需要区分的是，部分数据库提供的客户端侧列加密能力由数据库驱动在应用进程内完成加解密，明文暴露边界收敛于应用侧，并不属于 TDE，其密评判定应按“应用对数据资源本身进行加密”的要件另行核查。

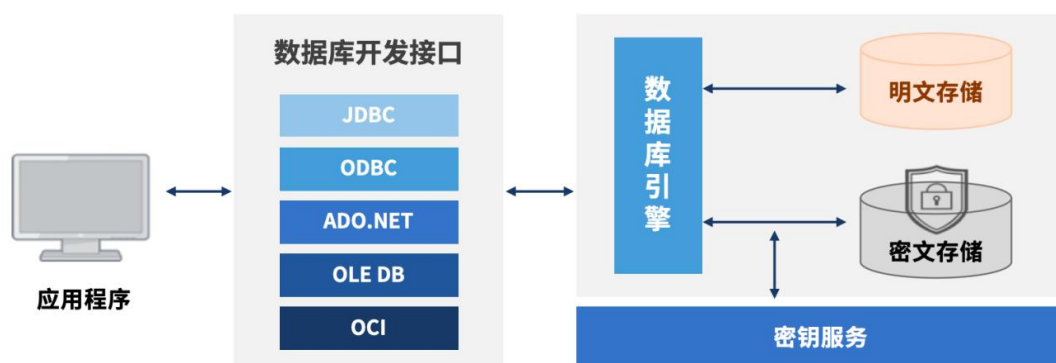


图 9 TDE 透明数据加密技术原理

2、应用场景

透明数据加密适用于需要对数据库静态数据实施整体保护，同时对业务改造量和查询性能有较高要求的场景，典型包括：

- (1) 需防范磁盘、数据库文件、日志或备份文件被窃取、脱机复制造成的数据泄露；

(2) 存量应用较多、不宜大规模修改应用代码，希望在不改变原有数据访问方式的前提下补做静态加密；

(3) 需要通过外部密钥管理系统或密码机加强密钥集中管理与密钥密文分离。在实际使用中，可借助 Oracle 等产品提供的密钥管理接口，将默认的软密钥钱包升级为外部密钥管理系统，以增强密钥安全性。

3、优势

(1) 对应用透明，改造成本低。加解密由数据库存储引擎完成，一般不要求应用修改原有的数据访问逻辑，存量业务系统补做静态加密的工作量较小。

(2) 性能损耗较低。加解密主要在数据库存储 I/O 路径中实施，不改变数据库引擎对 SQL 语句的解析、查询优化以及排序、关联、聚合等处理过程，数据库自身的性能特征得以保留，整体性能损耗通常较低，但具体影响仍与数据库产品、加密范围和业务负载有关，应通过实测验证。

4、挑战

(1) 保护边界有限，不具备防范 DBA 越权访问的能力。TDE 是落盘加密，数据在数据库内存中处于明文状态；数据库正常运行并取得密钥使用权限后，具有相应权限的数据库用户或应用仍可获得明文。因此原生 TDE 无法单独防范高权限账号、DBA 越权查询以及通过合法接口批量取数等风险，需与身份鉴别、细粒度访问控制、权限分离和安全审计配合使用。

(2) 数据库产品与版本适用性受限。TDE 由数据库厂商在产品内部实现，不同产品及版本在支持情况、加密粒度、算法、密钥管理接口，以及日志、备份、临时文件等对象的覆盖范围上存在差异，部分能力还受商业授权和部署环境限制。物理备份文件通常随 TDE 保持密文，但通过数据库正常接口逻辑导出的文件或数据已被解密，需另行采取加密和外发控制措施。

(3) 引入外部密钥管理会增加运维复杂度。对接外部密钥管理系统或密码机后，需统筹密钥授权、轮换、备份、恢复与容灾；密钥服务中断、密钥丢失或授权配置错误，可能导致数据库无法启动或历史数据无法解密。

(4) 密评定位：判定取决于是否配套细粒度访问控制。依据 FAQ 第四版第 23 条，TDE 属于数据整体加密实现的透明加解密：未采用细粒度访问控制时属第（1）种情况，需根据信息系统实际安全需求确定该技术手段能否有效应对系统面临的数据安全威胁；采用了基于身份鉴别的访问控制、不同用户数据隔离等细粒度访问控制措施时属第（2）种情况，可酌情判定密码使用有效性（D）为符合，并给出风险提示。由于原生 TDE 不改变数据库自身的身份鉴别与访问控制机制，其判定结论因而依附于系统另行具备的访问控制措施。

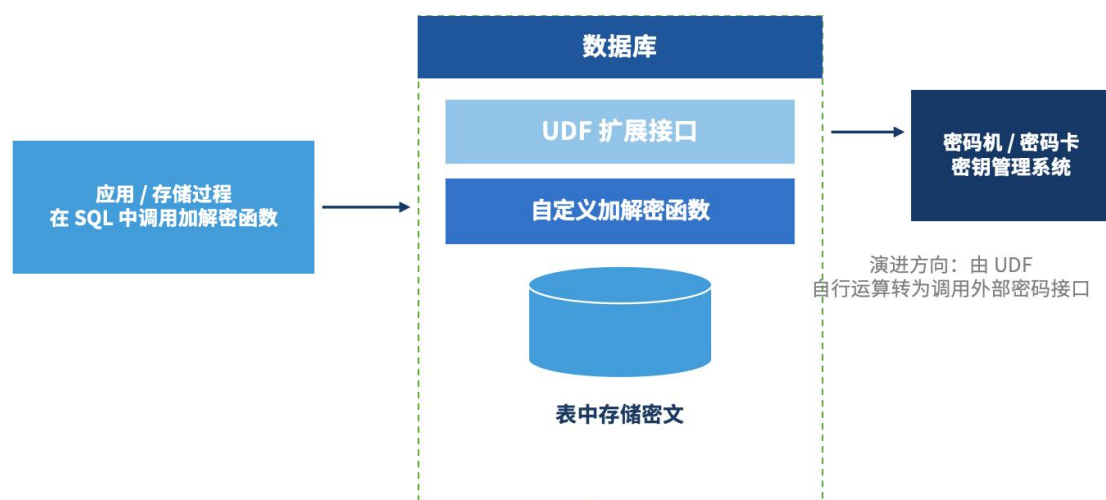
5、技术演进

TDE 的能力补齐主要发生在国产数据库与云数据库上，SM4 等商用密码（国密）算法被纳入支持范围，加密覆盖范围也从数据文件扩展到备份、日志和临时文件；同时，密钥管理正由数据库内置转向对接外部密钥管理系统、密码机与客户管理密钥，实现密钥与密文分离和主密钥集中轮换。推动这一进程的，主要是信创替代和密评对密钥全生命周期管理的要求。TDE 正在成为数据库的默认基线能力，而非差异化的安全产品。但能力普及不等于边界改变，数据库正常运行时，获授权的数据库用户与应用仍可获得明文。

技术八：UDF 用户自定义函数加密技术

1、原理解析

- 部署位置：数据库
- 原理：UDF 用户自定义函数（User Defined Function）是利用数据库提供的扩展接口，通过定义函数名称和执行过程扩展数据库处理能力。UDF 用户自定义函数加密，是通过 UDF 接口实现数据在数据库内的加解密。



早期实现中密码运算与密钥常写在函数内部，存在密钥硬编码与密码模块合规性问题

图 10 UDF 用户自定义函数加密技术原理

2、应用场景

UDF 用户自定义函数加密，作为一种在数据库侧的高灵活加解密集成方式，适用于某些数据库需要定制加解密的场景，尤其是实现基于国密算法的数据加解密。

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加解密处理。

(2) 单次改造范围可控，适合渐进式国密替换。采用本地密码卡时，加解密在数据库主机内完成，不引入网络跳数；对接网络密码机或密钥管理系统时，可实现密钥外置管理，但需评估逐行调用带来的网络交互开销。对既有系统的改动集中在需要加解密的字段所涉及的 SQL 语句和存储过程上，可按表、按字段分批推进，适合在版本稳定的存量系统中开展小范围、渐进式的国密改造。

4、挑战

(1) 通用性不足。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，并且在存储过程或 SQL 中加以调用。

(2) 密评定位：FAQ 第四版未专门规定。UDF 承载的只是算法调用与密钥对接的实现位置，其合规性仍取决于所对接的密码产品与密钥机制；加密动作仍在数据库侧由数据库进程完成，且需要在 SQL 或存储过程中显式调用，本质上仍属于对既有数据访问逻辑的改造。该形态介于应用侧加密与数据库侧加密之间，FAQ 第四版未就此作出专门规定，其是否构成“应用对数据资源本身进行加密”，需结合具体实现方式、密钥掌握方和配套访问控制措施，由测评人员综合核实后判定。

5、技术演进

UDF 加密的演进集中在两个方向。一是部分数据库将国密算法作为原生函数内置，同类需求不再依赖外部 UDF 开发，UDF 的使用场景相应收窄；二是 UDF 由自行实现密码运算，转向调用外部密码机、密码卡或密钥管理系统的接口，以解决密钥硬编码和密码模块合规性问题，但需要随数据库类型逐一定制、通用性低的固有局限依然存在。

技术九：TFE 透明文件加密技术

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 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，其实现可采用内核过滤驱动、文件系统模块或用户态文件系统等方式，部分方案可实现“逐文件逐密钥”加密。在正常使用时，文件内容进入内存后以明文形式存在，而保存在磁盘上的数据是密文；未获授权的主体与进程，读取到的始终是密文。

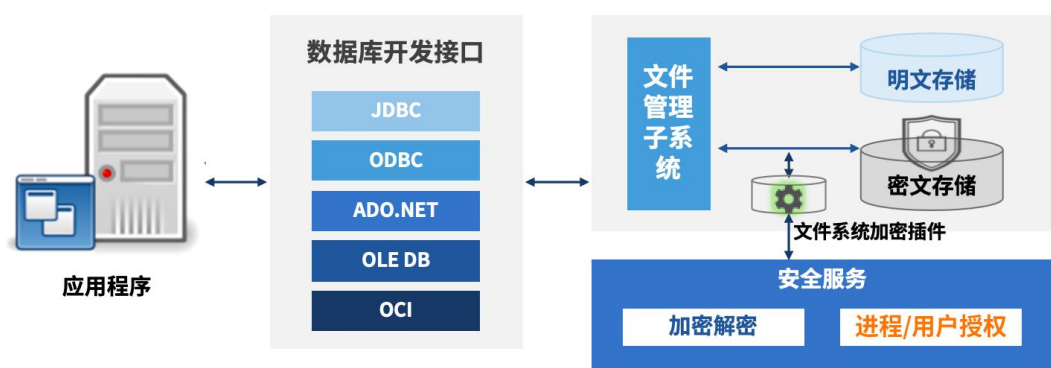


图 11 TFE 透明文件加密技术原理

2、应用场景：主要适用于文档、图片、日志等非结构化文件的静态加密。用于数据库数据文件，或涉及直接 I/O、内存映射、备份恢复的应用时，应验证文件系统、内核、数据库和存储硬件的兼容性与性能。

3、优势：可对应用进程授权。透明文件加密的防护粒度较细，可以适用于对应用进程有绑定需求的场景，只有授权的“白名单”应用进程访问文件时，才能获得明文，而未授权应用只能获取密文。

4、挑战

(1) 无法感知应用与数据库内部身份。TFE 的授权粒度止步于操作系统用户与进程：当数据库或应用进程被列入授权白名单后，DBA 及应用内用户通过正常接口访问数据时均可获得明文，TFE 无法在此层面实施细分控制。但对于系统管理员绕过授权进程直接读取文件的行为，仍可通过进程白名单机制将其限制为仅见密文。

(2) 高性能实现难度较大。透明文件加密会增加文件 I/O 路径中的加解密和策略判断环节，对文件 I/O 密集型业务的整体性能造成一定影响，实现高性能仍面临工程化挑战。

(3) 密评定位：判定取决于是否配套细粒度访问控制。TFE 以文件为单位实施透明加解密，属于数据整体加密实现的透明加解密：未采用细粒度访问控制时属 FAQ 第四版第 23 条第（1）种情况，需根据信息系统实际安全需求确定该技术手段能否有效应对系统面临的数据安全威胁；采用了细粒度访问控制措施时属第（2）种情况，可酌情判定密码使用有效性（D）

为符合，并给出风险提示。由于 TFE 的授权粒度止步于操作系统用户与进程，不能识别应用与数据库内部身份，该项配套措施通常需由系统的其他组件提供。

5、技术演进

透明文件加密正在分化为两条路线。一条是操作系统与文件系统原生化，以 Linux fscrypt 为代表，支持按目录策略派生逐文件密钥，并可借助块层内联加密硬件降低 I/O 开销，稳定性与性能占优，但授权主体是系统用户与密钥环，不提供按应用进程授权的能力；另一条是安全厂商的内核过滤驱动或用户态文件系统产品，保留进程白名单等细粒度授权语义，代价是需要持续跟随内核、数据库和存储硬件版本适配。

技术十：FDE 全磁盘加密技术

1、原理解析

- 部署位置：存储层
- 原理：全磁盘加密（Full Disk Encryption，简称 FDE）是对整个磁盘或卷中的数据实施整体加密的技术。加解密动作发生在文件系统之下，具体位置取决于实现方式：一类通过操作系统内核、块设备驱动或卷管理机制以软件方式实现，数据在写入磁盘前由主机侧的加密组件完成加密，读取时先解密再提交给文件系统和上层应用；另一类由自加密硬盘等存储设备内部的控制器以硬件方式完成，数据经主机侧下发至存储设备后，由设备自身完成加密并写入介质。无论哪种方式，磁盘或卷在使用前都需要先行解锁，通过口令、密钥、可信平台模块（TPM）或其他机制完成解锁后，加解密过程对操作系统、文件系统和应用程序都是透明的；设备关机、未解锁或存储介质脱离原系统时，磁盘上始终保持密文。



图 12 FDE 全磁盘加密技术原理

2、应用场景

- (1) 防范服务器、终端、移动设备或可移动存储介质丢失、被盗造成的数据泄露；
- (2) 防范磁盘、卷或虚拟磁盘被脱机复制、非法挂载和直接读取；
- (3) 设备报废、返修、转移或存储介质处置过程中，降低残留数据被恢复和利用的风险；
- (4) 需要在不改变文件系统和上层应用的前提下，对系统盘或数据盘实施整体静态数据保护。

3、优势

- (1) 保护范围较广。FDE 以磁盘或卷为单位实施，可覆盖位于该加密卷上的文件系统、应用数据、临时文件和交换空间；用于系统盘时还可覆盖操作系统相关文件，避免因遗漏特定目录造成明文暴露。
- (2) 性能损耗较低。FDE 对连续的数据块实施加解密，不介入文件系统和数据库的语义处理；在具备密码运算硬件加速或采用自加密存储设备的情况下，性能代价通常可控。
- (3) 部署实施相对集中。FDE 不需要逐一识别和配置文件、字段等数据对象，在保护目标和运行环境相对统一的终端、服务器或存储设备中，可集中配置、批量下发。

4、挑战

(1) 保护粒度粗，不具备独立的访问控制能力。FDE 以整个磁盘或卷为保护对象，无法按文件、数据库字段、业务用户或数据敏感级别实施差异化加密，也不提供独立于操作系统之外的数据访问控制。

(2) 难以防范系统运行期间的攻击与高权限访问。磁盘或卷完成解锁后，上层系统即可透明获得明文；一旦解锁口令泄露，或系统被漏洞利用、恶意代码入侵，FDE 无法阻止数据被读取、导出和复制，对系统管理员、数据库管理员等高权限账号同样无能为力。它真正应对的，是设备与存储介质离开受控环境之后的风险。

(3) 密钥与恢复机制管理要求较高。规模化部署时需统筹解锁口令、恢复密钥、TPM 绑定、密钥托管与设备更换等事项；恢复密钥丢失、TPM 状态变化或解锁配置错误，可能导致磁盘无法挂载、数据无法恢复。

(4) 密评定位：属第（1）种情况。依据 FAQ 第四版第 23 条，全磁盘加密属于数据整体的物理层加密存储，仅能防止设备或存储介质被窃取、复制导致的泄露，需根据信息系统实际安全需求确定其能否有效应对面临的数据安全威胁。由于磁盘解锁后上层系统即透明获得明文，FDE 自身不具备与加密对象对应的访问控制能力，难以通过配套措施进入第（2）种情况，不能仅凭启用 FDE 即认定符合应用和数据安全层面的要求。

5、技术演进

FDE 的演进体现为保护范围由本地磁盘和卷扩展到云上的虚拟磁盘、快照与镜像，并普遍支持客户管理密钥与外部密钥管理，密钥控制权部分回到数据控制方；随着密码运算硬件加速和自加密存储设备普及，性能代价进一步下降。需要注意的是，云盘加密由存储服务侧实施，与主机块设备层的 FDE 并非同一控制点，二者信任边界不同，不宜混为一谈。

表 1 十种数据存储加密技术特性对比

序号	加密技术	部署位置	加密粒度	明文暴露边界	密钥掌握方	性能	防 DBA	数据库复杂计算	实施成本	第 23 条对应情形
1	DLP 终端加密	终端	文件	授权进程内存	终端管理平台	中	/	/	中	(1) / (2)
2	CASB 代理网关	用户/终端-云服务之间	字段/文件	网关及用户侧	网关侧	中	条件支持	影响	高	视实现
3	应用内加密 (集成密码 SDK)	应用服务器	字段/文件	应用进程内(授权上下文)	应用侧/KMS	高	支持	影响	高	(3)
4	应用内加密 (AOE 面向切面加密)	应用服务器	字段/文件	应用进程内(授权上下文)	应用侧/KMS	高	支持	影响	低	(3)
5	数据库加密网关	应用服务器-数据库之间	字段	网关及上层应用	网关侧或外部 KMS	中	条件支持	影响	中	(1) / (2)
6	数据库外挂加密 (FGDE 细粒度动态加密)	数据库 (库内插件)	字段	数据库进程及授权主体侧	外部密钥管理系统	中	条件支持	不影响	低	(2)
7	TDE 透明数据加密	数据库	表空间/整库 (部分产品支持列级)	数据库内存及上层应用	数据库或外部 KMS	高	不支持	不影响	低	(1) / (2)
8	UDF 用户自定义函数加密	数据库	字段	数据库内存及上层应用	数据库、密码机或外部 KMS	中	不支持	影响	高	未专门规定

9	TFE 透明文件加密	文件系统	文件	授权进程及上层应用	安全服务或系统密钥环	中	不支持	不影响	低	(1) / (2)
10	FDE 全磁盘加密	存储层	磁盘/卷	解锁后全系统可见	设备/操作系统密钥体系（恢复密钥由组织托管）	高	不支持	不影响	低	(1)

注：“/”表示不涉及；CASB 行“防 DBA”指云服务商侧数据库/运维人员，与其他行所指的企业自身 DBA 不同。

注：“第 23 条对应情形”列依据 FAQ 第四版第 23 条给出。第（1）种情况指数据整体的物理层加密存储，仅能防止设备或存储介质被窃取或复制导致的泄露，需根据信息系统实际安全需求确定其能否有效应对面临的数据安全威胁；第（2）种情况指数据整体加密实现数据库透明加解密并采用了细粒度访问控制，可酌情判定密码使用有效性（D）为符合并给出风险提示；第（3）种情况指应用对数据资源本身进行加密并将密文写入数据库表、文件或对象存储，未解密时仅能查看数据密文，密码使用有效性（D）可判定为符合。标注“（1）/（2）”者，其具体归属取决于是否配套细粒度访问控制；“视实现”指是否形成存储密文取决于具体产品及配置；“未专门规定”见对应技术小节。需要强调的是，第 23 条判定的是加密实施主体、加密对象与配套控制措施，并不评价明文暴露边界与密钥控制权，落入同一情形的技术其实际防护效果仍存在差异，应结合本表相关维度综合分析。最终判定以测评机构结论为准。

十种数据存储加密技术在适用场景、优势与挑战上各有侧重。按典型控制点看，DLP 终端加密侧重终端文件保护；CASB 代理网关在加密或令牌化模式下可保护进入云服务的数据；应用内加密（集成密码 SDK）和应用内加密（AOE 面向切面加密）在应用侧对数据资源本身实施加密；数据库加密网关、数据库外挂加密（FGDE 细粒度动态加密）、TDE 和 UDF 作用于数据库访问或存储环节；TFE 侧重文件级静态数据，FDE 侧重磁盘或卷整体静态数据。技术选型不宜只看“是否有密文”，还应结合威胁场景、控制点位置、明文暴露边界、密钥控制权、查询功能、性能和运维条件分层组合。

从十种技术的演进轨迹看，有三条趋势值得关注。一是加密能力正在下沉为基础设施的默认配置。透明数据加密成为数据库的基线能力，国密算法被内置为数据库原生函数，云上虚拟

磁盘、快照与镜像普遍纳入加密覆盖。加密本身不再稀缺，价值随之转向“由谁掌握密钥、按什么规则释放”。二是控制点持续向应用侧前移，加密粒度同时向数据内部下沉。从磁盘、文件系统的整体加密，到数据库侧的落盘加密，再到应用侧对数据资源本身加密，控制点一步步逼近数据源头；加密对象也由整盘、整库收敛到表空间、逐文件乃至字段级。两个方向一前移、一下沉，实质都是让加密贴近数据本身的业务语义，而不是停留在承载数据的容器上。三是密钥管理正在超越算法选型，成为各条路线共同的瓶颈与分水岭。十种技术几乎都在向同一个方向演进：密钥由系统内置保管转向外部密钥管理系统、密码机与客户管理密钥；技术路线之间的差异在收敛，密钥治理能力的差距在放大，而这恰恰是密评考察的重点所在。

三条趋势最终汇聚到同一个判断：应尽量在数据写入数据库表、文件或对象存储之前，由应用侧完成加密并掌握密钥。无论是密码机硬件加密，还是应用层免改造加密，只要满足这一点，即具备 FAQ 第四版第 23 条第（3）种情况的判定基础；最终判定还需核查未解密时是否仅能查看数据密文，并结合所用密码产品的合规性、部署配置的正确性与密钥全生命周期管理的有效性综合认定，以测评机构结论为准。相较于依赖应用开发改造调用密码接口的方式，炼石应用内加密（AOE 面向切面加密）以“应用免改造”方式实现对数据资源本身的加密，是兼顾合规确定性与实施敏捷性的存储加密实现方式。对于应用侧改造不可行的存量系统，透明加密与 FGDE 细粒度动态加密在数据库侧组合，可提供第（2）种情况的判定路径，与应用侧路线并行互补。围绕密钥控制权与控制点前移两条主线，炼石结合国家法律法规及各行业监管要求，打造免改造数据安全产品平台，覆盖应用系统、数据库、文件系统、磁盘、终端等多个控制点，并面向大模型与智能体场景延伸运行时安全控制能力，持续强化以数据为中心的防护边界。

存储加密技术的选型路径

综合前述控制点划分与判定标准，存储加密的选型可按以下次序推进，每一步的结论都应可核查、可向测评机构说明。

第一步，确认系统定级与密评要求。对第三级及以上信息系统，重要数据存储机密性为无缓解措施的高风险项；依据《商用密码应用安全性评估管理办法》第九条，其运营者应当每年至少开展一次密评。

第二步，明确主要威胁场景。以介质失窃、脱机复制、勒索拷贝为主的，指向文件系统与存储层的控制点；以应用层越权、内部人员批量取数、特权账号越权为主的，指向应用侧控制点。

第三步，确定可接受的明文暴露边界。明确明文允许出现在哪些进程与环节，并据此反推控制点位置，而不是先确定产品再论证边界。

第四步，核定密钥控制权归属。明确密钥由谁掌握、按什么规则释放；需注意全磁盘加密、透明文件加密与数据库透明加密在运行期必须将密钥交付给操作系统或数据库进程，密钥控制权存在技术上限。

第五步，在既定边界内评估密文可计算性与性能。评估加密对模糊检索、排序、聚合等运算的影响与配套机制，并以实测数据替代厂商给出的相对评级。

第六步，组合部署并准备密评举证材料。按优势互补原则选择一种或组合多种技术，明确本方案对应第 23 条的哪一种情况，以及需向测评机构提交的密码产品合规性、部署配置正确性与密钥全生命周期管理有效性的证明材料。

附录 数据存储加密的另外五个分析维度

正文按加密控制点在数据流转路径上的位置，对十种存储加密技术做了归类比较；控制点影响了明文在哪里产生、密文在哪里形成，是最便于工程落地的分类方式。但它不是唯一角度：同样是数据库透明加密，密钥由数据库自持还是由数据控制方在外部掌握，防护效果与合规判定并不相同；同样是应用侧加密，密文能否检索、是否保留格式，直接影响改造成本与业务可用性。本附录列举五个控制点之外的分析维度，任何一种技术都可以在这五根轴上各自定位，没有在所有维度上同时占优的方案。

一、密钥信任边界：控制权的归属与演进

密钥控制权的演进路径清晰：由服务方全权托管，到客户主密钥、自带密钥，再到密钥始终留在客户自建密码设备中的外部密钥管理；最新形态是“凭证明释放”，由运行环境的远程证明结果决定是否下发密钥。需要注意两点：其一，控制权并非越外置越好，外部密钥管理引入的可用性风险通常需由用户自行承担，密钥服务中断会直接导致数据不可用；其二，密钥控制权存在技术上限，全磁盘加密、透明文件加密和数据库透明加密要正常运行，密钥必须交付给操作系统或数据库进程，运行期该进程始终可以获得明文，只有在应用侧或更靠近数据源头完成加密，才可能把明文与密钥边界收敛到数据库和平台运维之外。这也是表 1 中“密钥掌握方”与“明文暴露边界”两列需要合并阅读的原因。

二、密文可计算性：与明文暴露边界的反向取舍

密文可计算性，指数据加密存储后还能在多大程度上参与检索、排序、聚合等运算，取值从完全不可检索、仅支持等值匹配，到借助可信执行环境完成完整运算不等。它与明文暴露边界呈反向关系：加密越靠近存储介质，数据库运算越不受影响，但明文暴露边界越大，应用层越权访问、注入攻击无从防范；越靠近数据源头、粒度越细，存储机密性的判定确定性越高，密文参与运算的能力则越受限。因此可计算性高本身不构成技术优势，工程上正确的次序是先按威胁场景与合规要求确定可接受的明文暴露边界，再在该边界之内寻求尽可能强的可计算能

力。这一取舍也正是 FAQ 第四版对数据整体加密实现的透明加解密存储提出额外判定条件的原因。还需注意：保序类加密和确定性加密会泄露密文的顺序或分布特征，公开研究已表明可被有效攻击，不宜默认启用；全同态加密在通用数据库场景落地进展有限，不宜作为可预期的近期选项。

三、密文形态：标准密文、保留格式与令牌

细粒度加密落地的常见障碍，是密文长度和字符集与原字段不一致，牵动字段类型、校验逻辑和下游系统改造。保留格式加密使密文保持原有格式与长度，可直接写回原字段，但相关国际标准仍在修订过程中，选型应以最新标准文本为准；令牌化以无实际含义的替代值取代原值，令牌本身不承载可解密信息，可缩小合规审计范围，代价是需维护映射关系或承担派生计算开销。二者与细粒度加密方向一致，是使其规模化落地的工程手段；在密评场景下能否作为存储机密性的符合性证据，仍取决于所用算法、密码产品与密钥管理是否满足商用密码应用要求。

四、保护对象：加密什么

前述维度关注“怎么加密”，保护对象回答“加密什么”：存储加密的作用对象，正从数据库字段、文件、磁盘与卷、对象存储，延伸到列式文件，以及模型权重、嵌入向量与索引等新型数据对象。新型对象并未带来新的加密控制点，其加解密仍发生在应用或计算引擎进程之内，本质是应用侧加密向新载体的延伸；真正的差异在于配套机制——对象存储关注明文暴露边界能否收敛在应用之内、主密钥是否由数据控制方掌握，列式文件关注加密结构随文件跨平台流转而不失效，模型权重关注密钥按什么条件向运行环境释放，向量与索引则需评估检索过程本身是否泄露访问模式与语义信息。保护对象影响加密粒度的可选范围、密钥数量与配套能力设计，但不改变加密发生在哪一层。

五、算法生命周期：加密敏捷性与后量子迁移

存储数据的留存周期往往以年甚至十年计，而密码算法的安全强度会随计算能力和分析方法的进步而衰减，方案设计之初就应考虑算法与密钥的可替换性，即加密敏捷性。后量子迁移是当前最具体的体现：受量子计算直接威胁的是基于大数分解和离散对数的公钥算法，对称分

组密码通常以足够的密钥长度余量应对，并保持算法可替换能力；存储加密真正需要优先评估的，是包裹数据密钥的密钥加密通道、密钥管理系统的传输保护，以及长期归档数据所依赖的签名与时间戳。对留存周期长、敏感度高的数据，还应防范“先行留存、日后解密”的风险。迁移窗口应从数据的留存期限倒推，而不是从算法的禁用时点倒推。就国内实践而言，商用密码体系的演进与密钥管理系统的升级路径，需与这一迁移窗口统筹安排。

综合来看，控制点回答“在哪里加密”，密钥信任边界回答“谁能解密”，密文可计算性回答“加密之后还能做什么”，密文形态回答“业务系统要不要改”，保护对象回答“加密什么”，算法生命周期回答“这套方案能用多久”。实践中的多数争议，往往源于只在其中一两个维度上作比较，而忽略了在其余维度上付出的代价。建议在方案论证阶段逐一系列明六个维度的取值与理由，使技术选型依据可被复核，也便于在密评等合规场景中说明设计意图。

结 语

纵观各类技术，数据存储加密的选型并不是寻找一种能够覆盖所有场景的“标准答案”。加密离数据越近，明文暴露边界越小、合规判定越确定，但对密文运算、业务改造和密钥治理的要求也越高；离介质越近则反之。选型的实质，是在安全收益、业务影响与实施成本之间，建立与具体系统相适配的平衡。技术进入生产环境后，还要经受系统升级、权限变更、数据迁移、备份恢复和算法演进的持续考验。因此，数据存储加密不应被视为一次性改造项目，而应建设成为能够随业务变化持续调整、验证和更新的长期安全能力。

随着大模型和智能体加速应用，模型权重、训练语料、知识库、向量与索引、交互日志等新型数据对象不断进入保护范围，数据存储与数据使用的边界也在逐渐模糊。未来的安全治理将更加关注解密行为能否获得合法授权、解密环境是否可信、数据用途是否符合预期，以及调用、解密和输出过程能否被完整记录和追溯。细粒度保护、统一策略管理、密钥受控释放与加密敏捷，将逐步由单项产品能力演进为支撑智能化业务运行的基础能力。

面向这一趋势，炼石将继续完善以密码技术为核心的免改造数据安全能力，将数据加密、细粒度访问控制、密钥治理和审计追溯嵌入真实的数据处理流程，支撑结构化与非结构化数据、传统应用与智能化场景的一体化保护。让安全能力随数据进入业务流程，并在每一次调用、解密和输出中保持有效，既是炼石持续投入的方向，也是 AI 时代安全释放数据价值的重要基础。

公司介绍

炼石网络创立于 2015 年 2 月，是一家以“免改造”为创新特色的数据安全产品厂商，国家级专精特新“重点小巨人”企业，先后获得安天、国科嘉和、腾讯、重庆科技成果转化基金、朗玛峰创投、元起资本等投资。炼石已交付超五百家行业头部客户，产品已生产级部署在政府、金融、交通、电信、医疗、教育、工业、能源、商业等行业用户广泛的关键应用系统，当前实时保护着超千套应用、十多亿人口信息、数千亿条敏感数据，保障数据监管合规，促进数据有序流通。

炼石自研可灵活挂载多重安全能力的免改造数据安全产品平台，形成 AOE 面向切面加密、AOS 面向切面沙箱两大核心模块。AOE 面向 AI 重构中的重要网络与信息系统，保障核心数据、密码应用合规安全；AOS 面向大模型与智能体运行过程，强化权限控制、工具调用、跨域数据流转与远端推理可信。两大模块在统一平台下协同联动，形成从系统侧数据保护到 AI 侧运行控制的闭环安全能力，帮政企客户打造领先的数据安全保护体系，同时敏捷交付国密合规改造。

炼石多款产品获得商用密码产品认证证书、网络安全专用产品安全检测证书、涉密信息系统产品检测证书、通信网络安全服务能力评定证书；公司是国家互联网应急中心 CNCERT 首批数据安全支撑单位，入选工信部重点实验室成员、2023 年工信部、国家密码管理局“工业和信息化领域商用密码典型应用方案名单”和工信部“2020 年网络安全技术应用试点示范推荐项目”，荣获第十三届 ITEC 全球创业赛三等奖、北京市委网信办 IPv6 优秀案例三等奖等多项荣誉。公司通过 ISO9001、ISO27001、ISO14001、ISO45001 四项管理体系认证，持有北京市知识产权试点单位、北京市新技术新产品新服务证书，拥有 PCT 发明专利、数十项发明专利、近百项软件著作权及多项商标。

炼石免改造数据安全

北京炼石网络技术有限公司

BEIJING LIANSHI NETWORKS TECHNOLOGY CO.,LTD.



010-88459460



北京市海淀区四季慧谷·国家网络安全产业园48号楼2层



sales@ciphergateway.com

