白皮书

全密态数据库
第五代英特尔® 至强® 可扩展处理器
英特尔® 可信域扩展（英特尔® TDX）

英特尔® TDX 助力构建阿里云瑶池全密态数据库

阿里云

“云数据库已成为云计算时代管理数据的重要形态。阿里云瑶池数据库团队一直致力于为用户提供更快、更稳、更安全、更好用的云数据库服务。其中，保障数据安全始终是我们的第一要务。新兴的全密态数据库在确保全方位数据机密性的前提下，支持完整的 SQL 密文计算查询能力，已成为保障数据安全的利器。第五代英特尔® 至强® 可扩展处理器提供的英特尔® TDX 技术，让我们有机会构建更安全、更可信的全密态数据库服务，为用户的云上数据资产保驾护航。”

—汪晟
阿里云飞天实验室
数据库系统与安全负责人
阿里云瑶池数据库团队

“英特尔全新发布的第五代英特尔® 至强® 可扩展处理器全面支持英特尔® 可信域扩展（英特尔® TDX）技术，为客户提供面向虚拟化的机密计算新方案。英特尔® TDX 为云时代提供了坚实的安全保障，应用“零”修改，助力客户将基础设施即服务（IaaS）、平台即服务（PaaS）以及软件及服务（SaaS）等多类云应用轻松升级为机密计算模式。同时，英特尔® TDX 技术部署便捷，支持热迁移等云运维能力，方便客户构建高安全高可用的大规模机密云环境。阿里云瑶池全密态数据库结合英特尔® TDX，为用户数据安全提供了更强大的防御能力，为高安全性需求的云业务场景带来了明显的优势。”

—李志明
英特尔中国数据中心和人工智能集团 CTO

前言概述

在云计算和大数据时代，数据安全和隐私保护已成为全球热门话题。随着人们越来越关注数据安全和隐私保护，很多国家正在加强其数据保护法规，如欧盟的《通用数据保护条例》（GDPR）和中国的《个人信息保护法》（PIPL）。因此，企业在处理和存储用户数据时，需要更加谨慎和合规。在此背景下，全密态数据库技术应运而生。全密态数据库有助于为不同应用场景提供端到端的数据保护，帮助解决数据安全问题。阿里云瑶池全密态数据库结合英特尔硬件机密计算技术和阿里云安全防护能力，可以帮助有效防御来自云平台外部和内部的安全威胁，时刻保护用户数据。

英特尔全新发布的第五代英特尔® 至强® 可扩展处理器内置英特尔® 可信域扩展（英特尔® TDX）技术，为客户提供面向虚拟化实例的机密计算新方案。英特尔® TDX 提供了坚实的技术保障，助力客户在不改变现有应用程序的情况下，为其基础设施即服务（Infrastructure as a Service, IaaS）和平台即服务（Platform as a Service, PaaS）以及软件及服务（Software as a Service, SaaS）等多类云应用构建基于硬件设备的可信执行环境（Trusted Execution Environment, TEE），如机密虚拟机

或机密容器。同时，英特尔® TDX 技术使用便捷，能够帮助客户在云环境中大规模部署并实现实时迁移，拥有更灵活和友好的机密云计算环境。

基于硬件级别的机密计算数据保护

云环境中的数据按其所处状态，可分为三类，即传输状态 (Data in Transit)、存储状态 (Data at Rest) 以及使用状态 (Data in Use)。对于前两种状态，云服务提供商正借助安全访问、数据加密以及各类加密传输协议等技术来为客户打造更为安全可信的云端环境。而对于使用状态中的数据，机密计算是实现其有效保护的良策。机密计算为客户敏感数据提供了基于硬件的 TEE 环境，通过隔离保护的方式来帮助防止未经授权的入侵者访问或修改处理中的数据，从而成为了目前云服务中常见的、面向应用运行时的数据安全技术方案。

英特尔® 至强® 可扩展处理器机密计算方案

安全可靠的 TEE 技术

作为机密计算技术的重要引领者，英特尔推出了两种基于硬件级别的安全保护技术：英特尔® 软件防护扩展 (Software Guard Extensions, SGX) 技术，帮助提供软件级别的安全隔离保护；英特尔® 可信域扩展 (TDX) 技术，帮助提供虚拟化层级的安全隔离保护。凭借这两项内置的安全技术，第五代英特尔® 至强® 可扩展处理器能够帮助提供全面的机密计算能力，助力云服务提供商能够在基于硬件的可信执行环境 (TEE) 中，提供 IaaS、PaaS 和 SaaS 应用服务。

基于英特尔® TEE 技术，构建阿里云机密计算方案

英特尔® SGX 可以为应用程序建立一个可信边界，为用户提供一个安全可信的云上可信执行环境。阿里云很早就在其 ECS 云实例中引入了 SGX 技术。通过利用英特尔® SGX 提供的“飞地”(enclave)，阿里云为云应用建立了可信执行环境 (TEE)，帮助提高了应用程序使用中的数据安全。

此外，通过创建一个“信任域 (TD)”的虚拟机环境，英特尔® TDX 将客户操作系统和虚拟机 (VM) 应用程序与云主机、系统管理程序以及同一平台的其他虚拟机隔离开来。阿里云在第八代企业级 ECS 实例中集成了英特尔® TDX，成为首家在公有云中提供基于 TD 的机密实例和机密容器的公有云服务提供商。英特尔® TDX 为云上整个虚拟化实例 (包括虚拟机和云原生容器) 创建了一个可信赖的边界。因此，云终端用户可以创建一个机密计算环境，该环境将信任边界扩展到整个虚拟化实例，通过直接迁移 (lift-and-shift)，简化了传统应用程序向机密计算的迁移。

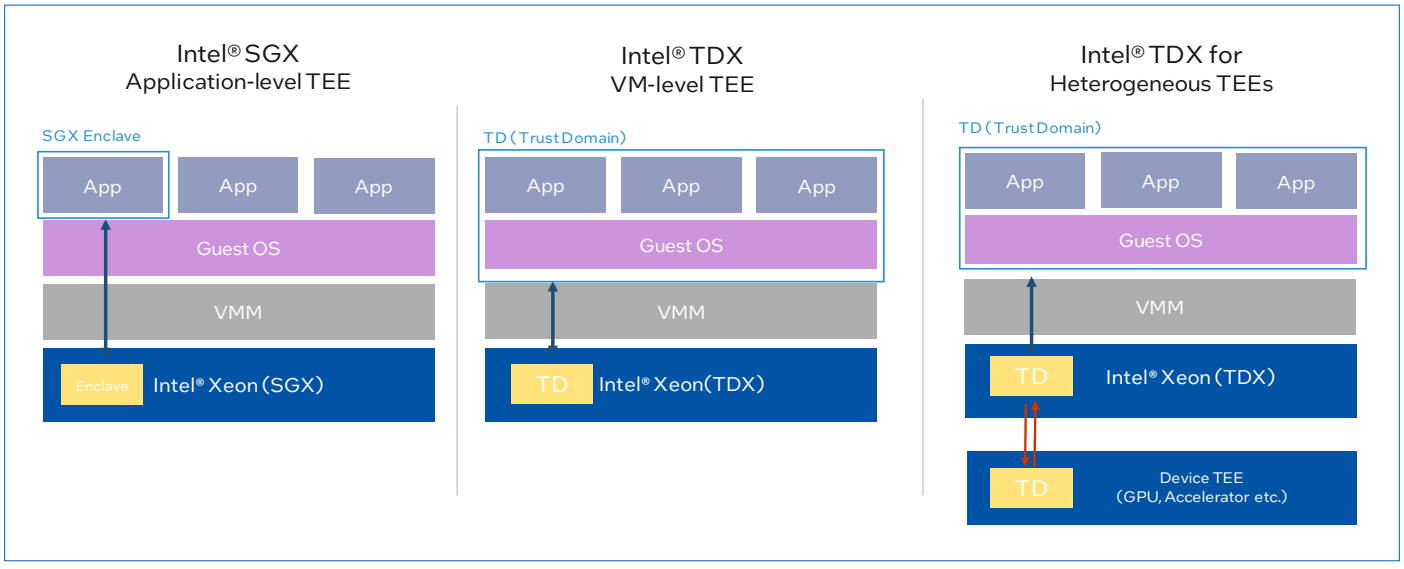

图 1. 英特尔® 至强® 可扩展处理器机密计算解决方案

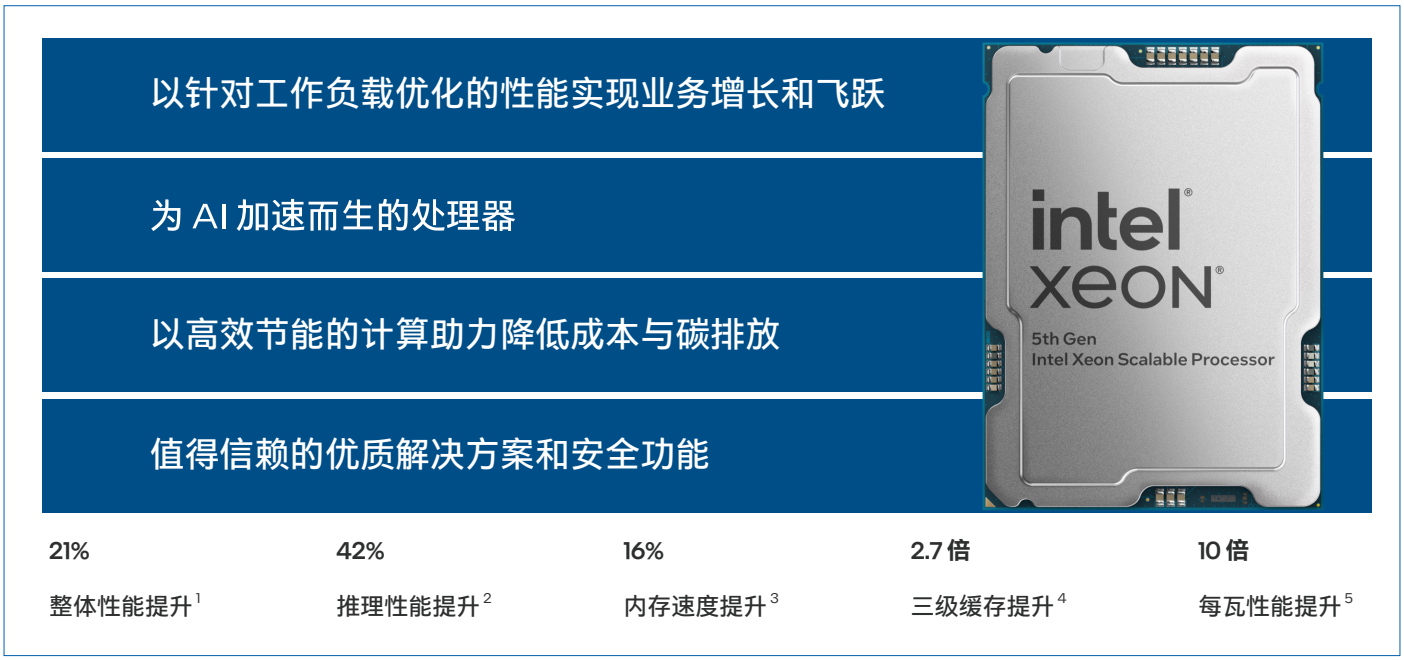

图 2. 第五代英特尔® 至强® 可扩展处理器具备更强大性能

基于英特尔® TDX 安全增强的瑶池全密态数据库

阿里云瑶池数据库基于全密态技术，保护用户敏感数据不泄露的同时，仍然支持所有的计算查询、事务等操作。相较于传统数据库针对数据所处阶段分阶段保护措施，例如 TLS (Transport Layer Security)、TDE (Transparent Data Encryption)、RLS (Row Level Security)，阿里云瑶池全密态数据库具备更强的数据安全防护能力。

数据库安全等级概述

从安全视角来看，不同云数据库防护安全威胁的能力不同，其安全性由弱到强可分为以下几个等级（等级越高，安全性越强）

- **常规云数据库：** 基于云安全服务，能够拦截绝大部分外部攻击，但仍然需要信任数据库实例内的操作系统、数据库软件、IaaS 运维人员、以及数据库用户。
- **基础安全数据库：** 在常规云数据库基础上，基于通用安全软件技术（如 SSL、TDE、动态脱敏等），拦截和保护租户数据，仅需信任数据库实例内的操作系统、数据库软件、IaaS 运维人员、以及高权限数据库用户。
- **全密态数据库（基础版）：** 结合全密态访问控制模块，限制数据库内数据库用户对数据操作的访问控制，避免非授权访问，可以帮助确保数据对包括 DBA 在内的任何数据库用户是可用不可见的，从而逐步实现数据私有化。仅需信任数据库实例内的操作系统、数据库软件、以及 IaaS 运维人员。
- **全密态数据库（硬件加固版）：** 在全密态数据库（基础版）的基础上，进一步基于 TEE 技术（例如英特尔® SGX/TDX），使得整个全密态数据库（基础版）服务运行在可信区域内，帮助隔绝任何数据库实例外部的安全威胁。仅需信任数据库实例内的操作系统、数据库软件。

[1] 与第四代英特尔® 至强® 处理器相比的平均性能提升，以 SPEC CPU rate、STREAM Triad 和 LINPACK 的几何平均值为衡量标准。请参阅 intel.com/processorclaims 上的 [G1]：第五代英特尔® 至强® 可扩展处理器。结果可能有所差异。

[2] 与第四代英特尔® 至强® 处理器相比，取得 1.19 倍到 1.42 倍的性能提升（ResNet50v1.5、BERT-Large、SSD-ResNet34、RNN-T（仅BF16）、Resnext101 32x16d、MaskRCNN（仅 BF16）、DistilBERT）。请参阅 intel.com/processorclaims 上的 [A15-A16]：第五代英特尔® 至强® 可扩展处理器。结果可能有所差异。

[3] 请参阅 intel.com/processorclaims 上的 [G12]：第五代英特尔® 至强® 可扩展处理器。结果可能有所差异。

[4] 请参阅 intel.com/processorclaims 上的 [G11]：第五代英特尔® 至强® 可扩展处理器。结果可能有所差异。

[5] 使用内置加速器在 AI、数据和网络工作负载上进行测量，取得 1.46 到 10.6 倍的每瓦性能提升。请参阅 intel.com/processorclaims 上的 [A19-A25]、[D1]、[D2]、[D5] 和 [N16]：第五代英特尔® 至强® 可扩展处理器。结果可能有所差异。

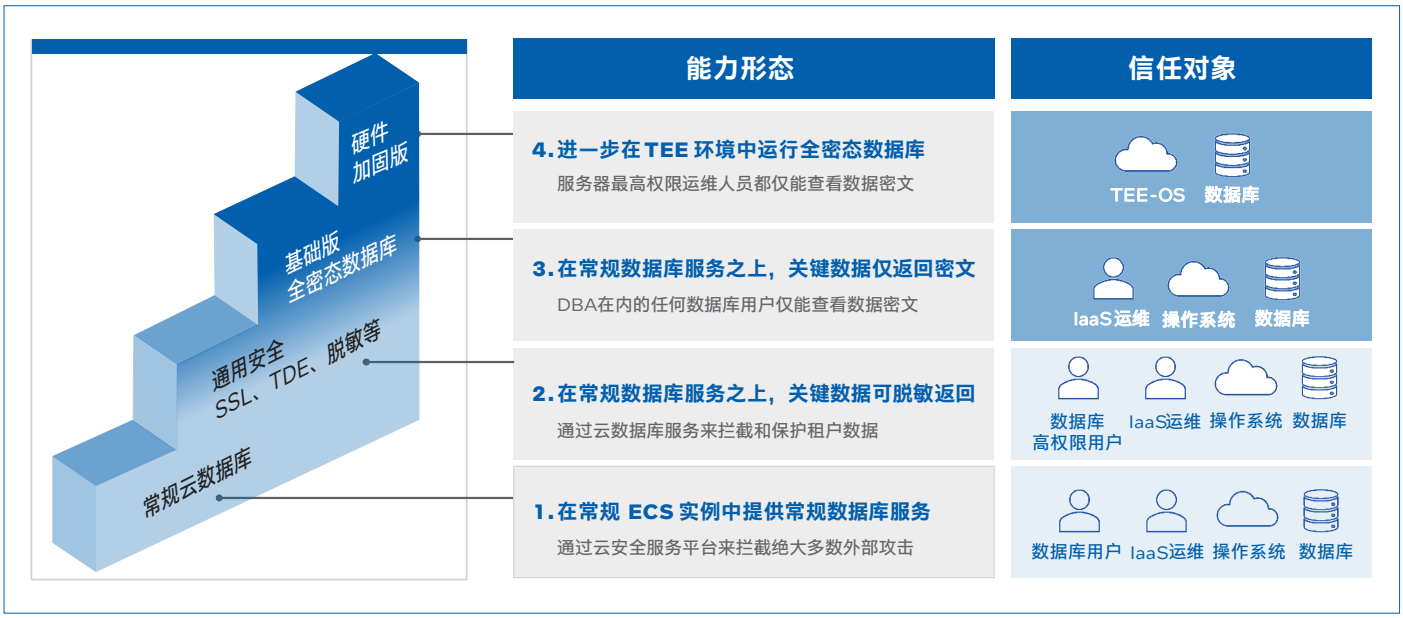

图 3. 阿里云瑶池数据库安全等级划分

全密态数据库采用机密计算能力，使得数据在非受信的服务器端全程以密文形式存在，但是仍然支持所有的数据库事务、查询、分析等操作，避免管理人员（如 DBA）以及其他非授权人员接触到明文数据，实现了数据在数据库内可用不可见。

阿里云瑶池数据库已正式发布 PolarDB MySQL[6] 和 RDS MySQL[7] 的全密态引擎（基础版）。同时，阿里云瑶池数据库与英特尔紧密合作，基于英特尔® TDX 技术构建硬件加固版全密态数据库，进一步增强数据库的安全等级。

阿里云瑶池全密态数据库基于英特尔® TDX 的受益

- 机密计算安全隔离：借助英特尔® 虚拟机扩展（Intel® Virtual Machine Extension，英特尔® VMX）技术与英特尔® 多密钥全内存加密（Intel® Multi-Key Total Memory Encryption，英特尔® MK-TME）技术，英特尔® TDX 为云实例提供了一种被称为“信任域（Trust Domain, TD）”的全新虚拟访客环境。TD 可与其它 TD、实例，以及底层系统软件、管理软件实现相互隔离。而这些安全策略的实施，是由运行在安全仲裁模式（Secure-Arbitration Mode, SEAM）下的 TDX 安全服务模块来完成。
- 加密内存数据流通性能优异：通过处理器中集成在内存控制器（IMC）的内置内存加密引擎，英特尔® TDX 帮助用户能够对传输中的敏感数据进行加密。这种方法消除了传统数据库在处理敏感计算时反复进行数据加密解密的额外开销。通过在基于英特尔® TDX 的可信执行环境（TEE）中运行数据库操作引擎，当云数据库处理用户敏感数据时，数据的状态可以得到机密保护。
- 便于大规模部署：直接迁移（lift-and-shift）简化了复杂的数据库系统向机密计算的迁移。此外，英特尔® TDX 还为超大规模部署提供了丰富的云操作能力，例如无服务中断的实时迁移和 TCB 升级。这些能力都降低了云上全密态数据库的操作和维护成本，提高了整体可用性。

[6] PolarDB MySQL：https://help.aliyun.com/zh/polardb/polardb-for-mysql/user-guide/confidential-engine

[7] RDS MySQL：https://help.aliyun.com/zh/rds/apsaradb-rds-for-mysql/feature-overview

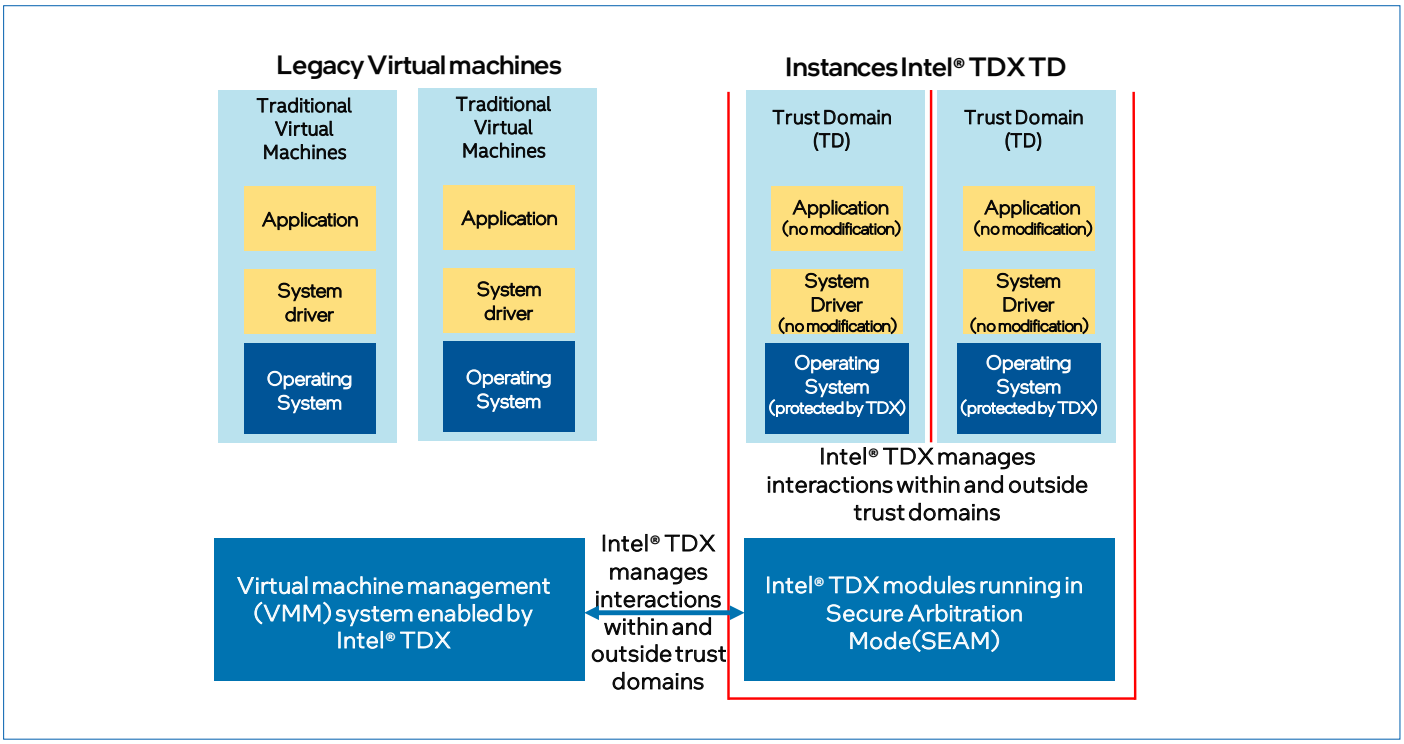

图 4. 英特尔® TDX 技术

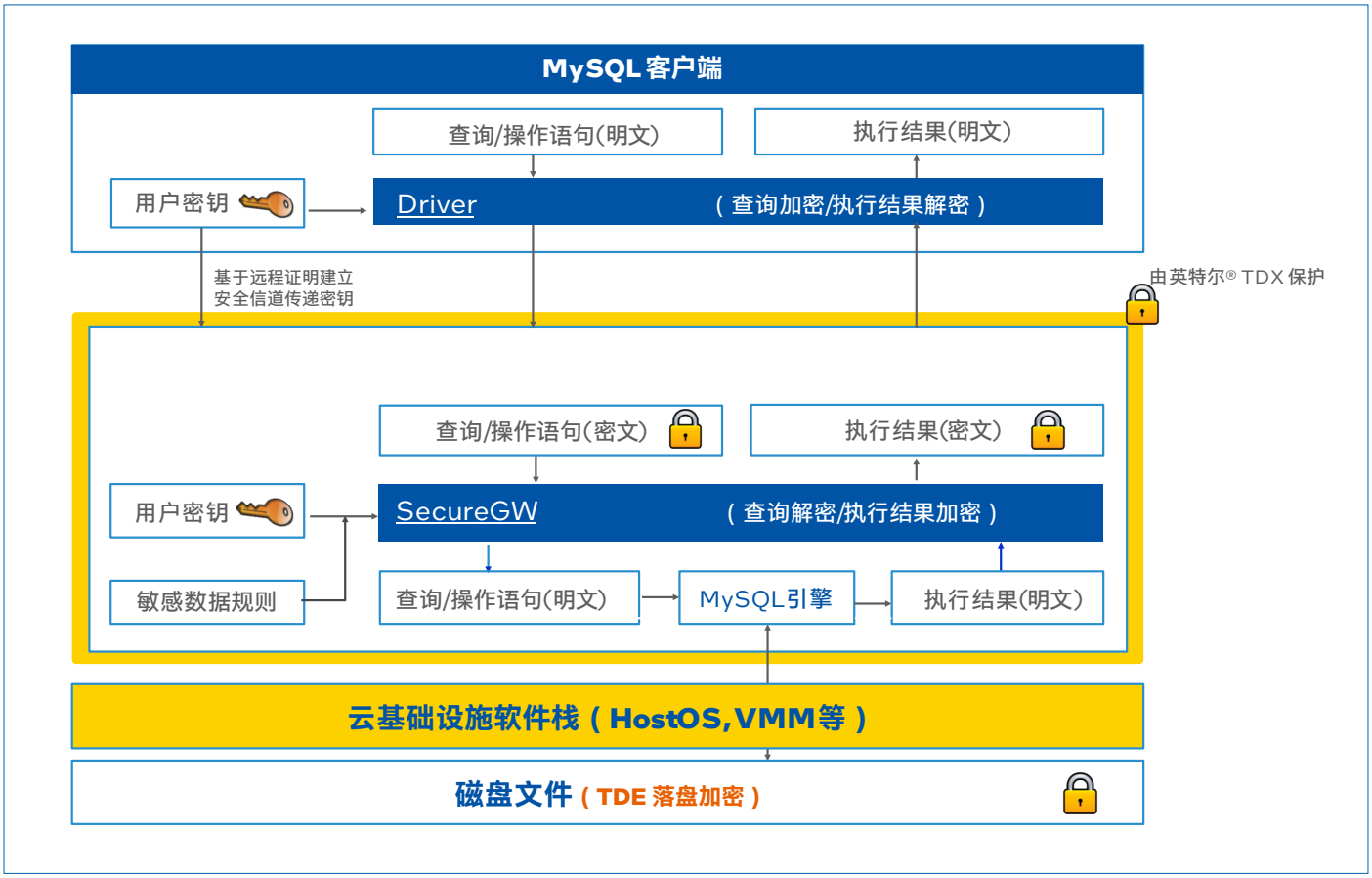

图 5. 阿里云瑶池数据库全密态 MySQL 引擎

用户接入阿里云瑶池全密态数据库后，查询的敏感数据始终以加密形式返回，即便数据库账号被盗数据仍不泄露。此外，瑶池全密态数据库采用英特尔® TDX 技术对数据库运行时内存加密保护，结合远程证明技术，提供端到端安全的密钥分发机制，无惧平台基础设施层的威胁。

此外，阿里云瑶池全密态数据库支持完备的 SQL 查询能力，兼容普通数据库，TPC-C 性能贴近明文性能；提供了对应用透明无感知的客户端接入方式，应用无需代码改造，同时支持数据传输服务（DTS）、数据管理服务（DMS）等生态工具，便于应用轻松迁移。

考虑到具备上述优势，阿里云瑶池全密态数据库能够为数据提供更强的保护，并更好地满足以下场景的安全需求：

- **平台运维安全**

在一般的应用场景中，数据的拥有者即为应用服务方。他们希望防止数据库服务及其运维人员接触到任何应用数据，同时保证数据库的正常运作。

- **数据安全合规**

在面向终端用户的应用场景中，部分数据（如健康数据、财务数据等）的拥有者为客户本人。他们希望应用服务只提供数据管理和分析的能力，不能接触私人明文数据，而应用服务也希望对敏感数据处理满足合规要求。

- **多源数据融合**

在进行多源数据联合分析时，他们希望保证在参与多方数据融合计算的同时，己方数据不会被其他参与方获取。

得益于英特尔® TDX 和阿里云瑶池全密态技术，对云数据库有高安全要求的用户可以采用阿里云瑶池全密态数据库系列产品，以实现卓越的数据安全保护。

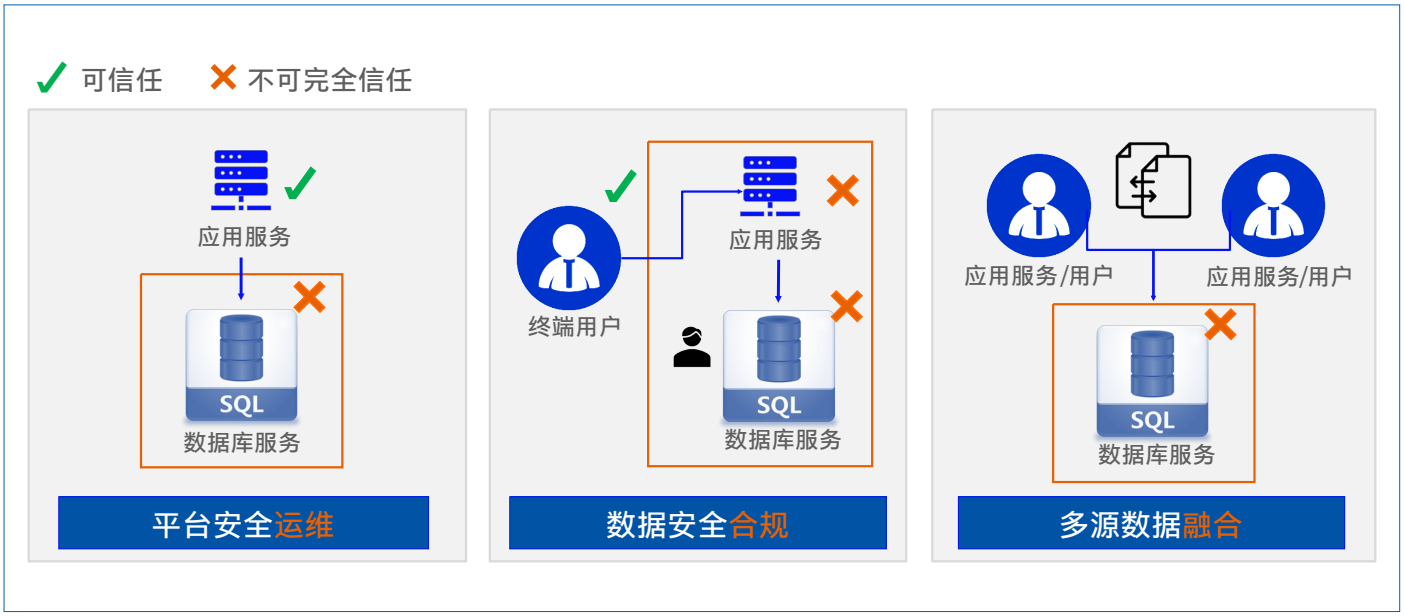

图 6. 全密态数据库典型应用场景

总结与展望

随着云服务安全关注度的不断提升，阿里云与英特尔都深刻地意识到，促进机密计算的技术发展和普及，应用和生态也是非常关键的一环。

确保客户数据的安全性和隐私性是云服务提供商的首要任务，而为客户提供有效的数据安全和隐私保护是阿里云所遵循的最重要原则之一。阿里云通过与英特尔合作，将英特尔® 至强® 可扩展处理器的机密计算能力融入 IaaS、PaaS 和 SaaS 中，为云终端用户提供丰富的数据保护和安全服务。阿里云瑶池全密态数据库结合英特尔® TDX，为用户数据安全提供了更强大的防御能力，为高安全性需求的云业务场景带来了明显的优势。

面向未来，阿里云还将与英特尔进一步展开深入合作，为更多行业和领域的客户构建更加安全、开放和高可靠性的云计算基础设施。

intel