产品简介

更高安全保障
英特尔® 至强® 可扩展处理器

内置英特尔® 安全引擎 助力创新加速，增强数据保护

内置英特尔® 安全引擎的第五代英特尔® 至强® 可扩展处理器可在维持出色性能的同时，加强对数据机密性与代码完整性的保护。

英特尔® 至强® 可扩展平台支持的机密计算可更好地保护使用中的数据

如今，对存储和传输状态下的数据进行加密处理已是行业的标准做法。然而，如何保护在处理器或内存中处于使用状态的数据，仍是企业面临的一大难题。在这种状态下，个人可识别信息、电子病历和金融交易等敏感数据存在较高的被利用风险、很容易发生意外暴露或违反合规要求。

在日益依靠数据驱动的世界中，企业需要保护其数据免遭未经授权的访问。英特尔® 至强®可扩展处理器配备多个英特尔® 安全引擎，可提供基于硬件的机密计算解决方案，让企业能够获得洞察、部署 AI 模型，并且在充分利用数据的同时更好地保护数据隐私。

借助第五代英特尔® 至强® 处理器，企业可以在处理器内创建安全飞地，并在其中对敏感数据进行处理和分析，从而避免将数据暴露给其他软件、合作方或云服务提供商。对于此前因过于敏感或出于监管原因而无法用于分析的数据，机密计算技术开辟了利用此类数据的多种可能。通过保护使用中的数据，第五代英特尔® 至强® 可扩展处理器还能帮助企业和机构履行隐私保护和合规义务。

这些安全飞地有助于保护使用中的数据免遭未经授权的访问。借助英特尔® 软件防护扩展（Intel® Software Guard Extensions，英特尔® SGX）和英特尔® Trust Domain Extension（英特尔® TDX），英特尔® 至强® 可扩展处理器可帮助客户选择更符合其业务和法规要求的机密计算技术。

借助英特尔® SGX 和英特尔® TDX，拥抱机密计算

由英特尔® SGX 提供支持的机密计算可实现应用或功能层面的数据隔离。无论是在云端、边缘还是本地环境，您都能确保自身的敏感计算与数据始终获得私密性和安全性更高的保护，不会暴露给云服务提供商、未经授权的管理员、操作系统和特权应用。

客户成功案例：英特尔® 至强® 可扩展处理器提供安全保障，助推创新进程

英特尔® 至强® 可扩展处理器正在助力 BeeKeeperAI 开发医疗领域的机器学习算法，同时加强对敏感数据的保护。数据管理专员可以利用英特尔® SGX 验证相关 AI 应用的完整性。

了解详情 ›

Zscaler 的云原生零信任交换平台（Zero Trust Exchange Platform）能够安全地连接任何地点的用户、设备和应用。Zscaler 将其零信任交换平台和应用连接器（App Connector）隔离在基于英特尔® TDX 的 TEE 中，并使用英特尔® Trust Authority 跨多个云基础设施验证其真实性和完整性。

阅读全文 ›

转型机遇无处不在

- AI 驱动的分析和服务
- 云经济及其规模效应
- 分布式应用和边缘应用
- 新数据源赋能服务创新
- 隐私保护技术
- 基于区块链的服务
- 围绕数据的多方协作

英特尔® SGX 经过深入研究和多次更新，是数据中心可信执行环境（TEE）的重要技术实现，能够大幅减少系统内的攻击面[1]。英特尔® 至强® 可扩展处理器的这一特性为在多个云和边缘部署机密计算解决方案提供了重要支撑。

英特尔® SGX 提供基于硬件的安全解决方案，可通过专用应用隔离技术帮助保护使用中的数据。开发人员可以通过保护选定的代码和数据不被查看或修改，在飞地内执行涉及敏感数据的操作，帮助提高应用的安全性和保护数据的机密性。

此外，英特尔® SGX 的认证功能让用户更加确信：运行在安全飞地中的软件完全符合各方的预期和既定规约。

英特尔® SGX 提供应用和功能层面的数据隔离，而英特尔® TDX 则在虚拟机（VM）层面提供隔离边界和机密保障。英特尔® TDX 可将客户机操作系统和虚拟机应用都与云端主机、虚拟机管理程序和平台的其他虚拟机隔离开来。虽然英特尔® TDX 的信任边界比英特尔® SGX 应用层面的隔离边界大，但英特尔® TDX 能使机密虚拟机比应用安全飞地更易于进行大规模部署和管理。英特尔® TDX 也为现有应用提供了一条更简便的向可信执行环境迁移的路径。与未启用英特尔® TDX 的第四代英特尔® 至强® 可扩展平台相比，基于启用英特尔® TDX 的第五代英特尔® 至强® 可扩展平台的虚拟机的整数运算、浮点运算和 BERT-large 性能可提升高达 11%[2]。

提高监管合规，加速数据分析

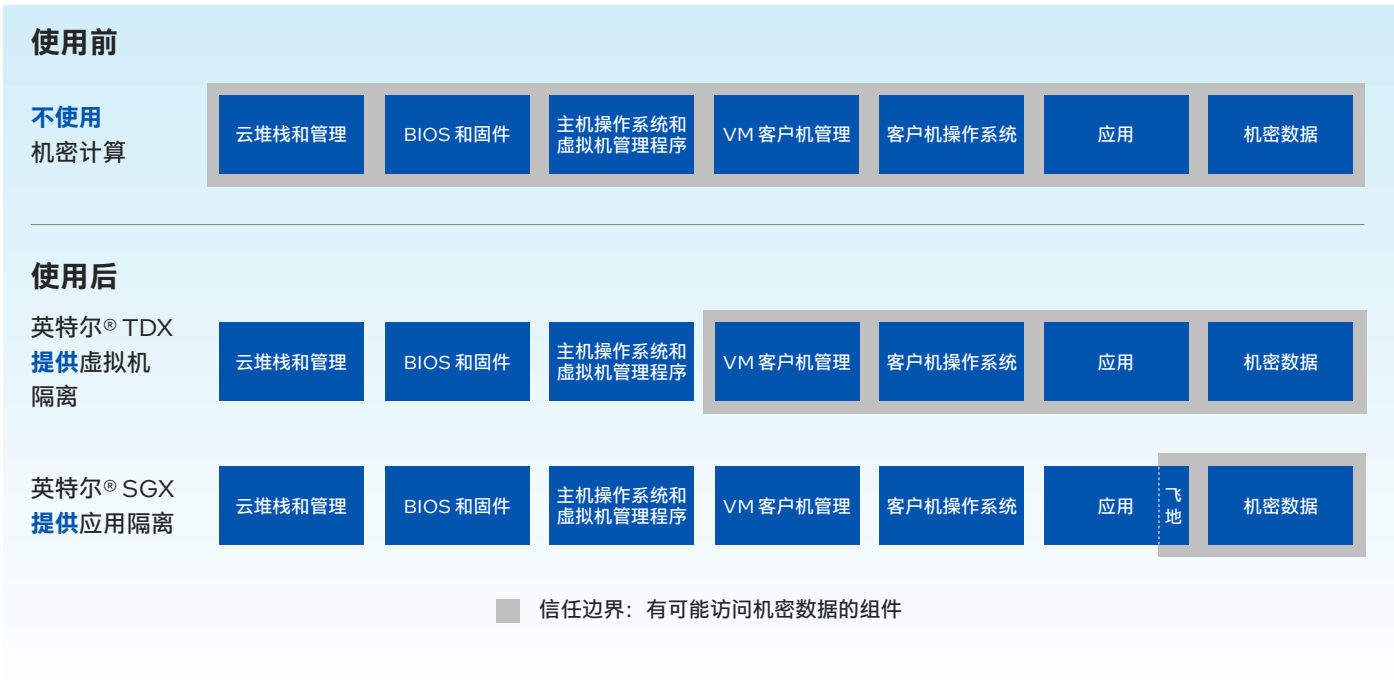
对企业有价值的数据经常受到严格的隐私法律法规约束。违反这些法律法规或会导致高额罚款和其他处罚，因此企业和机构会因面临风险而无法充分利用敏感数据。目前，在使用个人可识别信息方面，已有变通方法可用，但这通常会大幅减缓分析速度，甚至还会影响准确性。借助第五代英特尔® 至强® 可扩展处理器和英特尔® 机密计算技术产品组合，企业可以创建加密安全飞地，确保数据和应用的保密状态，从而改善合规状况，提升数据的可用性。

“鉴于 GDPR（《通用数据保护条例》）对数据泄露的处罚可高达全年总收入的 4%，数据保管人亟需增强对潜在受攻击面和使用中数据的保护。”

——机密计算联盟（Confidential Computing Consortium），2022 年 11 月[3]

克服敏感数据共享的障碍

在企业和机构间共享数据可以大幅提升神经网络训练等业务流程的准确性和速度。第五代英特尔® 至强® 可扩展处理器支持联邦学习等可信的多方计算模型，使共享机密数据成为可能。第五代英特尔® 至强® 可扩展处理器支持英特尔® 机密计算技术，能让多个参与方在无需将各自的私有数据暴露给未经授权的用户的前提下，汇集敏感数据，共享共同分析带来的益处。



利用英特尔® 密码操作硬件加速和英特尔® 数据保护与压缩加速技术，提升数据保护性能

如今，数据中心在保护数据的同时，除了传统边界防御，还依靠加密技术来保护网络传输、存储和数据压缩等进程。随着加密技术的发展，CPU 需要执行的加密周期数量也呈爆炸式增长，这可能对性能和用户体验带来潜在影响。

第五代英特尔® 至强® 可扩展处理器内置多项先进的加密加速技术，无需为数据中心增设更多内核或处理器，即可实现更高级别的加密安全性，提升性能并打造更加顺畅的用户体验。

英特尔® 数据保护与压缩加速技术（Intel® QuickAssist Technology，英特尔® QAT）是一项成熟的数据压缩和加密加速技术，作为内置加速器引入第五代英特尔® 至强® 可扩展处理器，用于支持动态数据压缩/解压缩和加密工作负载。通过卸载计算密集型工作负载，英特尔® QAT 可将更多内核容量释放给其他工作负载，同时有助于显著降低成本和压缩数据的占用空间[4]。

英特尔® 密码操作硬件加速指令采用更加严格的加密协议，例如更长的密钥长度、更强大的算法和更多的加密数据类型，以尽可能降低对用户体验的影响。通过使用更快的加密算法，用户不仅可获得性能提升和支持更高等级的服务级别协议（SLA），还可缩短计算周期，尤其是加密处理阶段的计算周期。

在算法层面，密码操作硬件加速技术主要通过加密计算的以下三个方面实现性能提升：

公钥加密： 针对安全套接字层（SSL）、前端 Web 和公钥基础设施（PKI）等用例。

批量加密： 针对安全数据传输、磁盘加密和流视频加密等用例。

哈希： 针对数字签名、身份验证和完整性检查等用例，例如安全套接字层所用的安全哈希算法 1（SHA-1）和安全哈希算法 2（SHA-2，也称 SHA-256）。

微软、SAP 和 Oracle 等公司所提供的多款商业软件包均已完成相关优化，可利用英特尔® 密码操作硬件加速。英特尔已对多款开源软件（众多 Linux 分发版、NGINX、Java OpenJDK Runtime 和 OpenSSL 库）完成优化，可支持英特尔® 密码操作硬件加速。

包括加密 API 工具套件（Crypto API toolkit）在内的开发人员工具可在英特尔® SGX 安全飞地内以更加安全的方式运行加密操作。此外，英特尔® 集成性能原语（Intel® Integrated Performance Primitives，英特尔® IPP）库还可自动使用可用的 CPU 资源，而面向 OpenSSL 的英特尔® QAT 引擎则可使网络安全软件解决方案以更加直接的方式，充分发挥英特尔® 密码操作硬件加速的性能。

您可借助英特尔® 至强® 处理器的内置加密加速技术，缩短加密处理阶段的计算周期，并提升企业的用户体验。

助力泰雷兹实现端到端数据保护

泰雷兹（Thales）与英特尔正协力普及机密计算，并在其 CipherTrust 数据安全平台（CipherTrust Data Security Platform）中加入数据保护功能，以更好地保护使用中的数据。英特尔和泰雷兹共同打造了一个可信的统一生态系统，为云端和本地环境提供全面的端到端数据保护解决方案，在解密客户敏感型工作负载之前认证环境的真实性。

借助由英特尔® Trust Authority 提供的可信认证，能够确保泰雷兹 CipherTrust 数据安全平台上的敏感工作负载不会在基于英特尔® TDX 或英特尔® SGX 的 TEE 以外被解密。泰雷兹的 CipherTrust 数据安全平台符合联邦信息处理标准 140-2（FIPS 140-2）等级 3。

这项技术有许多行业用例。例如，在医疗领域，利用患者数据集来训练机器学习模型，能够促进疾病诊断和药物开发。在银行领域，多家银行可以在不暴露个人信息的情况下共享数据，这有助于检测洗钱或其他异常交易。

在云端和数据中心建立广泛且可扩展的信任机制

第五代英特尔® 至强® 可扩展处理器配备多个英特尔® 安全引擎，在帮助企业利用云的灵活性和可扩展性的同时，能够降低暴露敏感数据的风险。英特尔® 至强® 可扩展处理器所支持的机密计算可将您的敏感数据与云服务提供商的软件、管理员和其他租户隔离开来。数据拥有者可通过远程认证功能，验证其安全飞地是否真实可信，是否处于最新状态，且只运行自身期望运行的软件。

选择英特尔® 至强® 可扩展处理器，挖掘更多数据价值

现在，通过全球范围内的云服务提供商和系统制造商，都可获得内置英特尔® 安全引擎的英特尔® 至强® 可扩展处理器。这些处理器不仅可为新服务提供支持，还可增加交易价值、防范金融犯罪、缩短研发周期，并推进涉及敏感、有价值或处于监管之下的数据的应用不断向前发展。

未来属于那些真正拥有并能充分利用好数据的人，英特尔® 安全引擎可助您早日成为数据王者。

进一步了解英特尔® 安全引擎如何为您业务中最关键的工作负载带来出色性能和安全保障。

机密计算 ›

英特尔® 安全引擎 ›

1. https://www.intel.cn/content/www/cn/zh/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html
2. 详情请见以下网址的 [S1]：intel.com/processorclaims（第五代英特尔® 至强® 可扩展处理器）。结果可能不同。
3. “Confidential Computing: Hardware-Based Trusted Execution for Applications and Data（机密计算：面向应用和数据的基于硬件的可信执行技术）”，机密计算联盟，2022 年 11 月，V1.3。
4. https://www.intel.cn/content/www/cn/zh/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html