产品简介

更高安全保障
英特尔® 至强® 可扩展处理器

英特尔® 安全引擎助力创新加速，增强数据保护

英特尔® 至强® CPU 配备多个英特尔® 安全引擎 (Intel® Security Engine)，可在维持出色性能的同时，帮助保护数据机密性与代码完整性。

英特尔® 至强® 可扩展平台支持的机密计算技术可在数据应用过程中确保数据隐私得到保护

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，企业在数据保护方面的薄弱之处却是数据在处理器或内存中处于使用状态时。在这种情况下，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。

使用机密计算技术，企业可利用敏感数据获得洞察，或者使用敏感数据进行 AI 模型训练，而不会将所用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和其他目的的数据，机密计算技术为企业开辟了利用此类数据的多种可能。

在基于双路英特尔® 至强® 可扩展处理器的服务器中，英特尔® 软件防护扩展（Intel® Software Guard Extensions，英特尔® SGX）飞地可处理高达 1 TB 的数据，因此为需要使用大型数据集的应用创造了更多机会。在完成训练或处理后，隐私信息都可在离开安全飞地前完成删除或重新加密。

基于英特尔® 至强® 可扩展处理器的安全技术，助您释放数据活力，更快向前发展

数据是推动创新与进步的源动力。从检测欺诈性交易到开发响应更迅速的供应链，再到训练具有突破性的 AI 模型，企业可利用数据完成各种各样的任务。可将数据转化为业务洞察的企业能走得更快、更远。

英特尔® 至强® 可扩展处理器的内置安全技术为各种数据（包括敏感、保密和处于监管之下的数据）保驾护航，使其可用于分析，进而帮助企业加速创新步伐。英特尔® SGX 是英特尔的独有技术，能够帮助保护使用中的数据。使用英特尔® 至强® 可扩展处理器的企业不必从数据分析和 AI 模型中剔除敏感数据，而是可通过英特尔® SGX 创建访问受限的数据安全飞地。这样的隔离环境可帮助企业在确保敏感数据始终处于保密状态的前提下，充分发挥其价值。

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层面、虚拟机（VM）、容器和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、未经授权的管理员和操作系统，甚至是特权应用。

英特尔® SGX 经过广泛部署和研究，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。

英特尔推出英特尔® Trust Domain Extension（英特尔® TDX），进一步提升保护级别。这一全新工具将于 2023 年开始通过特选云服务提供商为企业在虚拟机（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、系统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。

英特尔的机密计算技术产品组合在英特尔® SGX 和英特尔® TDX 加持下，允许企业选择他们需要的安全级别，以满足自身的业务需求和监管方面的要求。

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® SGX 和英特尔® 至强® 可扩展处理器帮助**全英房屋抵押贷款协会（Nationwide Building Society）**针对演进的“了解客户”（KYC）法律法规，简化合规流程。

了解详情 ›

宾夕法尼亚大学利用英特尔® 至强® 可扩展处理器和英特尔® SGX 优化 3DResUnet 肿瘤分割模型。测试结果：肿瘤边缘检测精度明显提升。

阅读全文 ›

机密计算的选择

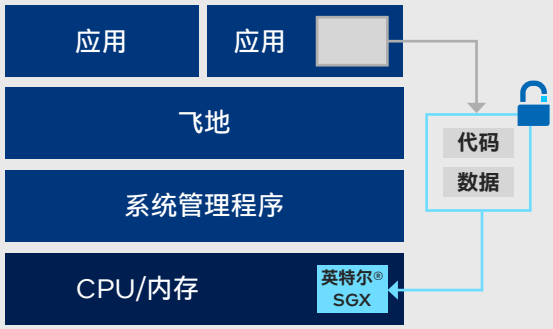

图 1. 英特尔® SGX 通过将敏感数据隔离在容量高达 1 TB 的飞地中，帮助保护敏感数据。

英特尔® SGX 用例

人工智能（AI）/机器学习（ML）
使用 AI 和 ML 处理敏感或处于监管之下的数据，同时改善隐私法律法规的合规状况。

云基础设施
严格限制服务提供商或其他公有云租户对您私有数据的访问。

可信的多方计算/多方分析
支持多方在云端就共享数据开展协作，确保敏感数据始终处于保密状态。

安全密钥管理
使用安全飞地保护密钥并提供类似硬件安全模块（HSM）的功能。

区块链
增强交易处理、共识机制、智能契约和密钥存储的隐私性和安全性。

网络功能虚拟化（NFV）
为虚拟化网络功能建立信任机制。

利用英特尔® 密码操作硬件加速增强安全性，提升数据保护性能

如今，除了传统边界防御，数据中心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。

第四代英特尔® 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，作为全新的内置加速器引入第四代英特尔® 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，同时显著降低成本和压缩数据的占用空间[2]。

英特尔® 密码操作硬件加速（Intel® Crypto Acceleration）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[3]，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：

公开密钥加密：在安全套接字层（SSL）、前端网页和公开密钥基础设施等用例中，公开密钥的加解密速度可提升高达 6 倍[4]。

批量加密：在安全数据传输、磁盘加密和流视频加密[6] 等用例中，使用英特尔® 高级矢量扩展 512（Intel® Advanced Vector Extensions 512，英特尔® AVX-512）可将加密的速度和性能提升高达 4 倍[5]。

哈希：在数字签名、身份验证和完整性检查等用例中，例如安全套接字层（SSL）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），安全哈希性能可提升高达 2 倍[7]。

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）加密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® 可扩展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，提升开发人员的敏捷性，优化 DevOps 效率，并提升企业的用户体验。

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，例如欧洲的 GDPR（《通用数据保护条例》）、美国的 HIPAA（《健康保险携带和责任法案》）和中国的 PIPL（《个人信息保护法》）。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，例如煞费苦心的匿名化处理，但这项耗时耗力的工作会大幅减缓分析速度，甚至还会影响准确性。借助英特尔® 至强® 可扩展处理器和内置的英特尔® SGX 技术，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。

“到 2023 年，个人信息受现代隐私法律法规监管的全球人口比例将由当前的 10% 增加到 65%。”

—Gartner[8]

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准确性，加快神经网络训练等流程。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。使用内置英特尔® SGX 安全飞地的英特尔® 至强® 可扩展处理器，多个参与方就能够汇集敏感数据，共享共同分析带来的益处，而无需将各自的私有数据暴露给彼此。英特尔® SGX 的认证功能让我们更加确信：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。

助力博世跨越安全难关

英特尔携手工程技术领导企业博世和软件创新品牌 Edgeless Systems 全力加速博世自动驾驶辅助项目的开发进程。为训练计算机视觉模型，博世使用了车辆未来行驶的街道和地点的真实视频与图像。由于此类视频片段包含面部图像、车牌号等处于监管之下的个人可识别信息，因此需要经过匿名化处理，以便博世的工作人员对其进行访问。然而，对数据进行匿名化处理常常会降低 AI 训练数据的准确性。借助英特尔® SGX，博世可在英特尔® SGX 数据的安全飞地中使用原始实时视频片段训练模型，在提升训练速度和训练结果质量的同时，始终做到遵守数据隐私法律法规。

在云端和数据中心建立广泛且可扩展的信任机制

英特尔® 安全技术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® SGX 等安全功能的英特尔® 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，并推进使用敏感、有价值或处于监管之下的数据的应用不断向前发展。未来属于那些拥有数据的人。英特尔® 加速引擎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。

英特尔–机密计算

intel® XEON®

[1] 英特尔® 软件防护扩展保护数据

[2] https://www.intel.cn/content/www/cn/zh/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html

[3] 英特尔解决方案，“Tapping into Cryptographic Acceleration”（掘金于加密加速），https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[4] 英特尔解决方案，“Tapping into Cryptographic Acceleration”（掘金于加密加速），https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[5] 英特尔解决方案，“Tapping into Cryptographic Acceleration”（掘金于加密加速），https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[6] 英特尔解决方案，“Tapping into Cryptographic Acceleration”（掘金于加密加速），https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[7] 英特尔解决方案，“Tapping into Cryptographic Acceleration”（掘金于加密加速），https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[8] “Gartner 表示，到 2023 年，个人信息受现代隐私法律法规监管的全球人口比例将达 65%，”Gartner，2020 年 9 月，gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w。