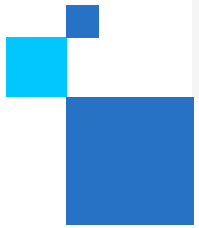
2023 年 11 月

机密计算 ISV 支持程序包

系统集成商 (ISV) 如何利用采用英特尔技术的解决方案，应对客户的业务挑战



何谓机密计算?

何谓机密计算?

使用机密计算技术，企业可利用敏感数据获取洞察或训练 AI 模型，
而不会将所用数据暴露给其他软件、协作者或云服务提供商
对于此前因过于敏感或受到监管而无法用于分析和其他用途的数据，
该技术为企业利用此类数据创造了多种可能

预计**机密计算**软件细分市场将成为**最庞大且增长最快的细分市场**，紧随其后的是硬件和服务细分市场

在短短数年内，**机密计算已获得广泛关注和迅速发展，可为使用中的代码和数据提供强大的全新端到端保护**

机密计算不可或缺
填补数据保护连续性方面的重大空白

静态数据	传输中的数据	使用中的数据
存储加密	网络加密	保密计算

Everest Group®

据 Everest Group 称，该“**数据安全的下一个前沿**领域……**将呈指数级**增长。”
2021 **年，全球市**场规模为 19 亿美元，预计到 2026 **年，在云和安全**项目的驱动下，复合**年增**长率将高达 40% - 95%。

保密计算

领域和使用案例

领域

使用案例

保密计算
关键 AI 用例

多方机器学习

在不影响客户敏感数据机密性和隐私性的情况下充分利用机器学习的强大功能

业务简介

在以下领域，利用机密计算进行多方机器学习特别有用：

医疗保健

可利用数据的力量进行**更多高**级研究，而不会**暴露机密的患者信息**

金融服务

可以更准确地预测潜在**欺**诈活动，同时还可打击**洗**钱和恐怖主义融资

客户案例研究

医疗保健

利用受监管数据进行协作计算

BeeKeeperAI™ NOVARTIS

情况

Novartis Biome 开发了罕见病诊断模型和疗法。罕见病信息较为稀少，且分散在多家医院和研究机构中

挑战

患者信息属于隐私且受到严格监管。医院不希望将数据转移到外地，也不想将私人档案披露给 BeeKeeperAI 或 Novartis

解决方案

每家医院本地安装的支持英特尔® Software Guard Extensions（英特尔® SGX）的 BeeKeeperAI 节点，将分析私人数据并更新云端的主模型权重。Novartis 和 BeeKeeperAI 人员均无法查看或存储受监管的健康记录

BeeKeeperAI™

“利用[机密计算平台]，我们可以将验证算法的周期缩短一半。它还将成本几乎降低了一半。这些节省有助于我们更快训练、验证可推广算法并将其推向市场。而且，随着 CCP 底层技术和流程日益成熟，它只会变得更加快捷、成本更低。”
MaryBeth Chalk，BeeKeeperAI, Inc 联合创始人兼首席商务官

白皮书

加速临床人工智能算法的发展

客户案例研究

高度安全的密钥保护

Fortanix®

情况

快速扩散的密钥和证书需要强大的保护和集中管理。
HSM 解决方案成本高昂，云解决方案依赖 CSP 安全和合规

挑战

利用与 HSM 类似的安全功能构建基于软件的可扩展密钥管理系统，该系统在技术上与其云主机相互隔离

解决方案

Fortanix 基于英特尔® SGX 构建了其自我防护型 KMS 软件，以防止密钥和证书受到外部对手和云提供商攻击并帮助确保所有者的机密仍受其控制

Fortanix®

通过启用英特尔® SGX，始终保持高性能
实施多实例配置可显著提高吞吐量。通过启用英特尔® SGX，可将对这些性能增强功能的影响降至最低，意味着组织可以同时提高安全性和性能。

解决方案速览

[机密人工智能数据英特尔安全解决方案 - Fortanix]

中国客户案例研究

挖掘数据价值

创邻科技

情况

如何确保企业数据和隐私安全是数据库和硬件制造商面临的常见问题

挑战

传统数据加密技术只会加密硬盘存储和网络传输，其效率以服务器控制权限未发生泄漏为前提。如果服务器控制权被拦截，第三方就可以窃取或修改使用中**的数据**

解决方案

利用英特尔® SGX **内存加密**，创邻科技**与英特尔**联合推出了一个图形数据库数据**加密解决方案。它可保**证 Galaxybase **的极致性能，从而**创建内存安全图形**数据**库产品

人们相信，在英特尔® SGX **内存加密技**术的帮助下，创邻科技创建的新一代图形数据库 Galaxybase **可**为客户提供高质量、**更加安全的数据服**务，有效实现数据互联，并助力企业稳定实现数据资产的价值。

新闻稿

英特尔提供哪些机密计算功能

英特尔提供全面的安全产品组合

英特尔® Software Guard Extensions（英特尔® SGX）

应用程序隔离

英特尔® Trust Domain Extensions（英特尔® TDX）

虚拟机隔离

英特尔® Trust Authority

面向多云和混合云的独立信任验证服务

软件解决方案、云、原始设备制造商和系统集成商生态系统

英特尔安全第一的开发和生命周期支持

*英特尔® TDX 通过特定云提供商提供

英特尔可信执行环境

应用程序级隔离：英特尔® SGX

优势

- **与云提供商和其他租**户分离
- **更小的信任**边界和潜在攻击面
- **更易于代**码检查和监控
- **可部署在虚**拟机、云原生容器和裸机中

考虑因素

- 应用程序可能需要专门开发或定制
- **安全隔区外部的**频繁调用可能会影响性能

虚拟机级隔离：英特尔® TDX

优势

- **与云提供商和其他租**户分离
- 现有应用程序的移植工作量最低
- **更符合企**业范围的部署要求
- **可以是**简单的实例配置器设置

考虑因素

- **更大的信任**边界（客户机操作系统、所有应用、**虚**拟机管理员）
- **更新的客**户机操作系统和管理程序可能需要**重新**验证
- 鉴证的精细程度降低

英特尔® Trust Authority

通过私有云安全，让零信任触手可及并获得公有云灵活性

英特尔® Trust Authority 是一个新的软件和服务组合，通过零信任原则为机密计算带来增强的安全性和保障
英特尔® Trust Authority 的第一代提供了独立的鉴证服务，可对基于（英特尔® SGX）和（英特尔® TDX）的
可信执行环境 (TEE) 进行鉴证。

在构建您自己的鉴证服务不产生成本和复杂性的情况下实施零信任原则

了解详情

机密计算支持包

产品简介

Noname 案例研究

Thales 案例研究

Zscaler 案例研究

概念视频

英特尔® Trust Authority
如何运行

开始使用英特尔® Trust Authority

1

- 设置或向您的云基础设施提供商请求基于英特尔® Software Guard Extensions（针对工作负载）或英特尔® Trust Domain Extensions（针对虚拟机 (VM)）的机密计算环境 (TEE) 实例

2

- 确定并实现要在这些机密计算环境中运行的工作负载
- 这可以在应用程序级别使用英特尔® SGX（通过 Gramine 或其他客户端库简化）或在虚拟机级别使用英特尔® TDX 来完成

3

- 订阅以获取英特尔® Trust Authority 认证密钥
- 将密钥插入工作负载（英特尔® SGX）或虚拟机（英特尔® TDX）上的客户端库，以便它可以直接与 SaaS 通信来验证 TEE

要注册英特尔® Trust Authority，请访问 intel.com/trustauthority 或联系 trustauthority@intel.com

了解有关英特尔® Trust Authority 安全解决方案的更多信息

保密计算

面向英特尔® Software Guard Extensions 的软件和解决方案生态系统

商业支持解决方案 — **自行构建**

商业解决方案提供商

anjuna
cosmian
CYBERNETICA
decentriq
EDGELESS SYSTEMS
Fortanix
Mithril Security
Opaque
enclaive
SCONTAIN
HUB SECURITY
secretarium

可即时部署的精选容器 (至 2023 年第一季度) *

PyTorch
redis
scikit learn
Spark
TensorFlow

开发人员工具

GRAMINE
SCONE
Occlum
Mystikos
Teaclave
Open Enclave SDK
intel
Intel SGX SDK

系统集成商

accenture
KPMG
Capgemini
IBM
Atos
leidos
avanade

管理程序 (SGX)

KVM
5.13 及更高版本
vmware
vSphere 8

* 可从 Azure Marketplace 获取

英特尔® TDX 可用性

英特尔® TDX 通过三家领先的云提供商在公开预览的第四代英特尔® 至强® 可扩展实例中提供

点击下面的标志了解有关每家云提供商的产品的更多信息

Microsoft Azure　Alibaba Cloud　Google Cloud

IBM Cloud
*公开预览待定

以下客户机操作系统供应商支持英特尔® TDX

Red Hat　SUSE　Canonical Ubuntu

*英特尔® TDX 将在 2024 年上市的第五代英特尔® 至强® 可扩展处理器中全面提供

怎样入手

英特尔® Software Guard Extensions（英特尔® SGX）

更多信息　　立即行动

云服务提供商
单击标志了解更多信息

Azure　CORE　OVHcloud　phoenixNAP GLOBAL IT SERVICES
swisscom　IBM Cloud　CloudSigma

原始设备制造商
单击标志了解更多信息

Hewlett Packard Enterprise　SUPERMICRO

培训和文档

培训视频　　技术资料库　　解决方案简介

英特尔® Trust Domain Extensions（英特尔® TDX）

更多信息

文档

面向开发人员的信任域安全指南

立即行动

英特尔® Trust Domain Extension（英特尔® TDX）模块下载

英特尔® Trust Domain Extension（英特尔® TDX）加载器

竞争性比较

	英特尔® Software Guard Extensions	英特尔® TDX	AMD SEV-SNP	AWS Nitro Enclaves	配置比较（在 NVIDIA H100 GPU 上）
云基础设施提供商的硬件/固件、管理程序以及云管理堆栈均被排除在信任边界以外	●	●	●		●
通过多家云提供商供货，以促进多源供应	●	●[1]	●		●
旨在通过低移植或无移植、重新设计或重新包装来适配旧版应用		●	●		◎[2]
验证硬件真实性和正确启动 TEE	●	●	●	●	●
验证在 TEE 中加载的软件映像的完整性	●	◎[3]	◎[3]	●	
机密数据只能通过指定的应用代码访问；虚拟机管理员、访客操作系统、其他应用和云堆栈均被禁止访问	●				
可部署到“裸机”服务器上，而无需虚拟化	●				●
基于硬件的加密内存完整性选项提供了额外的 Rowhammer 保护	●				
兼容代号为“Amber 项目”的英特尔独立信任服务	●	●			
竞争性数据源，截至 2023 年 3 月			链接、链接	链接、链接、链接	链接

[1] 英特尔® TDX 实例将于 2023 年通过部分云提供商上线；上市时间会有所不同
[2] 无需或少量更改在 GPU 上运行的旧版代码。一部分使用 CPU 的工作负载需要集成基于 CPU 的 TEE 和保护 PCIe 通信的方法。
[3] 并非可用硬件技术的固有功能，但可作为云或鉴证服务提供商提供的增值功能。

为什么选择英特尔进行机密计算?

为什么选择英特尔进行机密计算?

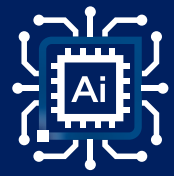
满足多样性安全需求的技术选项

只有英特尔能够同时提供应用隔离（英特尔® SGX）和虚拟机隔离（英特尔® TDX）功能，以便客户针对不同安全等级精确调整解决方案

广泛的解决方案生态系统

英特尔与数十家 ISV 和云提供商合作，共同提供托管服务和软件解决方案，包括机密 AI、分析、区块链、数据库等

联系英特尔专家和我们的解决方案合作伙伴



英特尔专家将随时为客户提供帮助，完成解决方案架构、合作伙伴匹配、POC 资源和部署故障排除等任务

联系 PSAM 了解更多信息

后续步骤

教育

了解机密计算的重要价值，以**及**许多最终用户应用如何利用**它来确保其**环境的安全并启用**多方**计算

互动

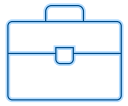
与您的英特尔 PSAM 联系，了解有关生态系统内的英特尔机密计算技术产品组合的更多信息

英特尔® 合作伙伴联盟如何提供帮助

开始使用英特尔® 合作伙伴联盟

成为英特尔® 合作伙伴联盟会员即可获得专属业务发展机会，例如进入我们的全球市场、高级培训和促销支持，所有这些均根据您的需求定制

培训和能力

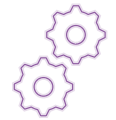


加入英特尔® 合作伙伴培训计划可获得有关高级技术、能力课程计划和学习奖励方面的专业培训

营销资源

进入英特尔解决方案市场和英特尔营销工作室，可帮助为您的产品和服务创造更多需求

有价值的奖励



通过参加符合条件的活动赚取积分，提升您的会员等级，并访问其他资源以拓展业务

如果还不是会员
立即加入

会员享有的权益

赢取积分

英特尔® 合作伙伴联盟中最受欢迎的独有权益之一，我们将向合作伙伴奖励积分，以对他们与英特尔一起取得的业绩以及积极参与高优先级活动做出表彰。

在英特尔® 合作伙伴联盟内，会员可通过 1,000 多种方式赚取积分，并兑换 100 多种奖品。

Cloud Insider 社区

英特尔® Cloud Insider 社区可提供不断更新的世界一流的云内容和工具。会员有机会与同行和生态系统建立联系，将创新型联合云解决方案推向市场

了解详情

行业洞察

黄金会员和钛金会员可访问精心策划的季度行业洞察，以帮助推动自身增长

了解详情

经济激励措施

会员可获得市场开发基金和激励计划的强大支持，以帮助您快速成功地进行产品营销

与您的 PSAM 交流，了解英特尔® 合作伙伴联盟加速器计划以及更多财务激励措施

intel partner alliance

如何获得客户支持

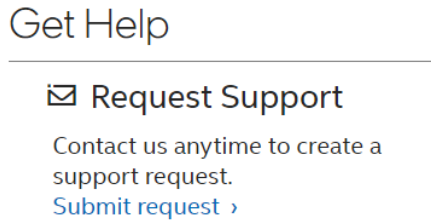
英特尔 Virtual Assistant

这个聊天机器人位于每个合作伙伴联盟网页**的右下角，提供可解答大多数**问题的自助**服**务或实时支持代理的快速链接。

获取帮助“Blade”

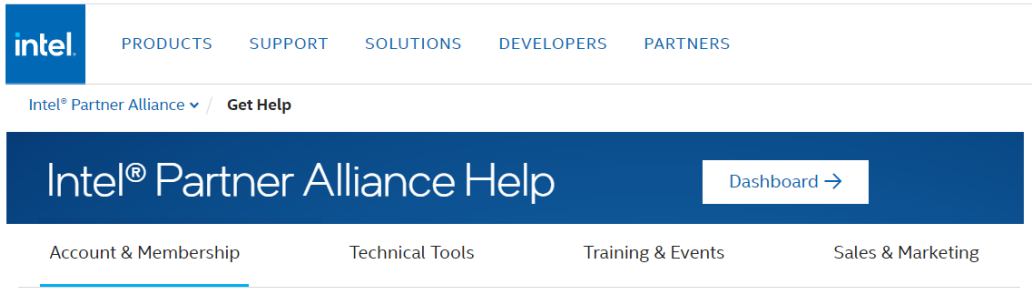
提交在线支持请求。

此链接位于合作伙伴联盟网站内大多数页面的页脚处。



合作伙伴联盟“获取帮助”页面

获取帮助页面提供了有关合作伙伴联盟成员可用的**大多数工具和**权益的详细自助指南。



资源

Cloud TV

英特尔® Cloud TV 将提供云计算新闻、趋势和战略，
助力您取得成功

云端的 Sapphire Rapids

了解如何保护您的云资产

云安全性

云端的安全挑战

云解决方案架构师认证

完成 CSA 课程表，用有关云实例详细信息、主题和解决方案的专家级知识武装自己

本课程表面向在云端实施解决方案拥有至少两年经验的云解决方案架构师进行了优化

您将获得的优势

巩固与云技术和解决方案架构相关的知识和技能，以增强设计和实施云解决方案的能力。
通过学习专为在线培训设计的交互式课程，加深对最新行业趋势的了解。这类课程便于学习者按自己的进度取得进展，并最大限度地降低对其工作和个人时间的影响。
跨一系列云工作负载通过基于云的 CI/CD 流水线，进行容器编排、AI 工作负载和实例优化，从动手实验中获得高深知识，深入了解高级云应用。
通过参加线上/监考考试获得行业认可的认证和证书。

立即开始自定进度的在线认证培训

保密计算
信息和资源

30-3-30

机密计算 30-3-30

技术文章

机密计算的现状

云安全简介

视频

机密计算概述

安全性面临挑战

博客

性能和网络安全的新范式

安全性从英特尔开始

研究论文

保护新兴 AI 工作流程中的
数据和模型

保密计算
面向开发运维人员和云架构师的资源

技术论文

利用机密计算加速 AI 推理

运用英特尔® Security Engine 加速创新，加强数据保护

白皮书

新增 如何防范云安全威胁

新增 通过机密计算实现主权着陆区

新闻简报

英特尔开发人员专区新闻简报

社区

英特尔社区

安全社区合作伙伴

视频

英特尔安全加速器视频

更多资源

性能指标

第四代英特尔® 至强® 可扩展处理器

直播线上研讨会

云解决方案架构师 (CSA) 技术讲座：利用第四代英特尔® 至强® 可扩展处理器降低总拥有成本并提高效率

线上研讨会录像

云解决方案架构师 (CSA) 技术讲座：利用第四代英特尔® 至强® 可扩展处理器加速关键工作负载

其他培训

能力课程和认证

机密计算
培训链接

安全培训链接

课程/培训

主题 - 受众
提高网络安全恢复能力的三项关键技术 开发运维人员、云架构师 – 机密计算
物联网解决方案的端到端安全性 开发运维
边缘到云端安全性 开发运维人员、云架构师
虚拟私有云、云联网和云安全性 开发运维
英特尔® 产品和解决方案的安全价值 全部
保护云中的应用程序 开发运维
云计算安全性 开发运维人员/云架构师

主题 - 受众
虚拟私有云、云联网和云安全性 开发运维人员、云架构师
业务对话的安全性 云架构师、高管
英特尔架构的加密入门 开发运维
英特尔® 产品和解决方案的安全价值 开发运维人员、云架构师

安全培训链接

在线教程

主题 - 受众
如何启用英特尔® Hardware Shield 安全功能 安全运维 - 端点安全性


intel