November 2023

Confidential Computing:

Addressing critical business challenges with Intel based solutions

What is Confidential Computing?

What is Confidential Computing?

Confidential Computing allows for the extraction of insights or training of AI models using sensitive data without exposing that data to other software, collaborators or your cloud provider

This provides an array of possibilities for businesses to harness data that was previously too sensitive or regulated to activate for analytics and other purposes

The **confidential computing** software segment is expected to be the **largest** and **fastest- growing market segment** followed by hardware and services

In just a few short years, **confidential computing has gained wide attention and momentum as a powerful new way to provide end-to-end protection of in-use code and data**

The Need for Confidential Computing

Closes a major gap in the Data Protection Continuum

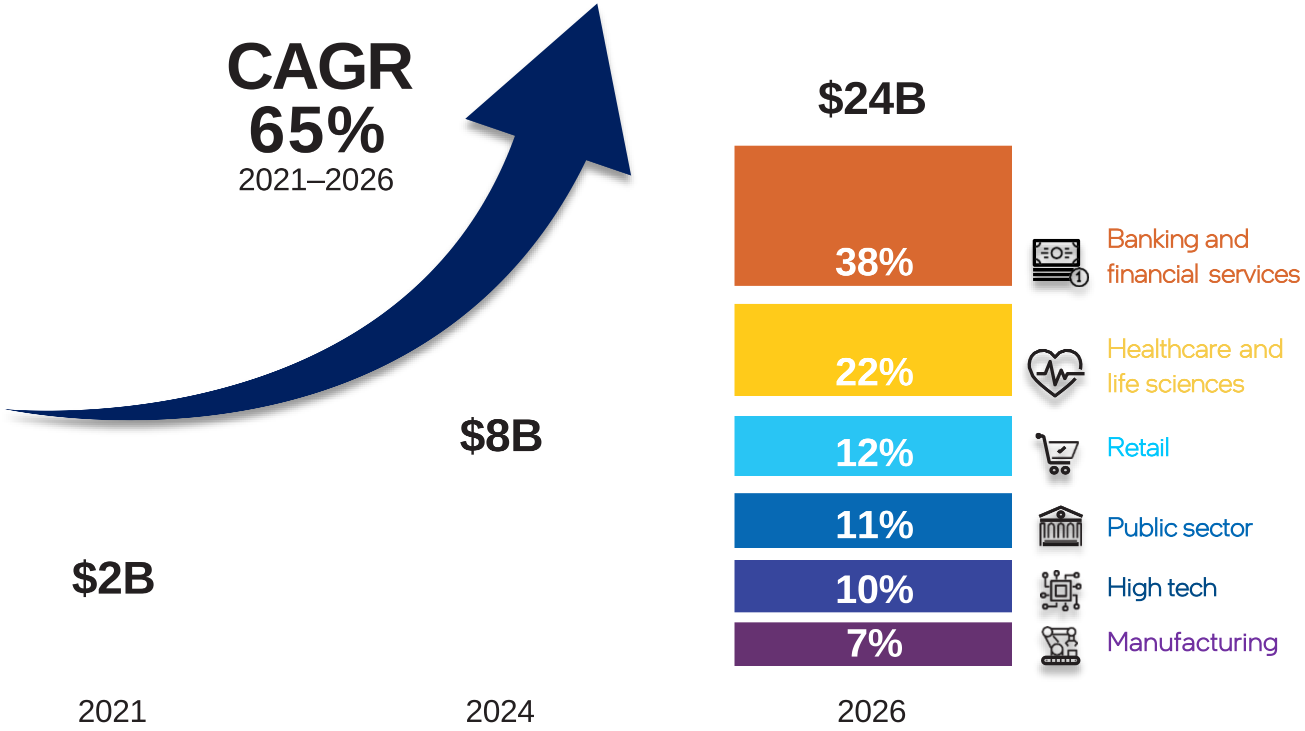
Data at Rest	Data in Transit	Data in Use
Storage Encryption	Network Encryption	Confidential Computing

Everest Group®

According to the Everest Group, this "next frontier in data security … is poised for exponential growth." The global market, $1.9 billion in 2021, is expected to grow at a compounded annual rate of 40% - 95% through 2026, driven by cloud and security projects.

Confidential Computing Market Forecast

Expected to Grow Exponentially, Driven by Cloud Security and Privacy-Preserving Multiparty Computation



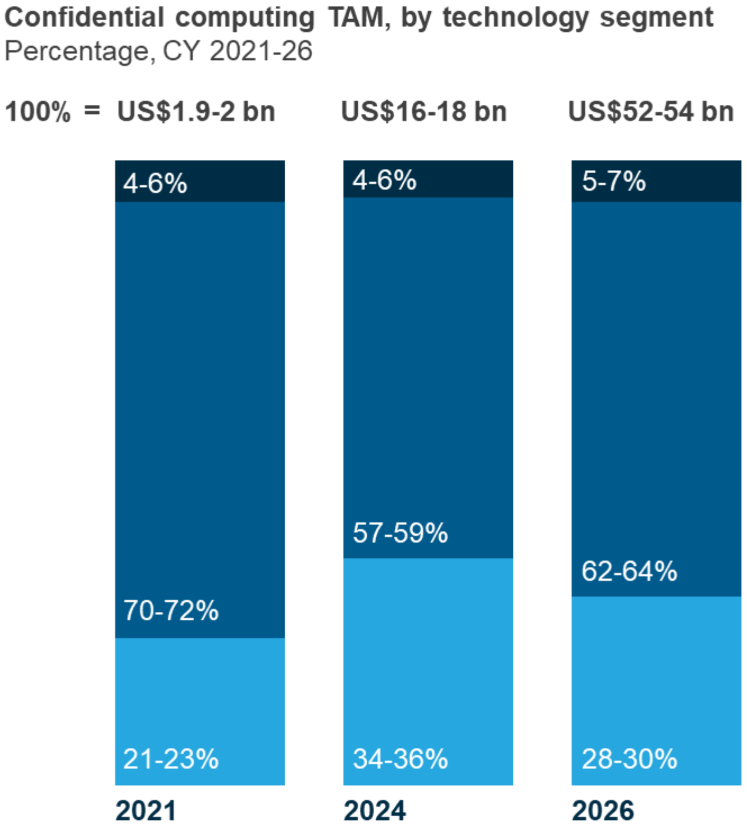
IDC MARKET INSIGHT

Source: 2021 Confidential Computing Consortium

Confidential Computing Market

The confidential computing software segment is expected to be the largest and fastest- growing market segment followed by hardware and services

Confidential computing TAM, by technology segment
Percentage, CY 2021-26



▇ Hardware ▇ Software ▇ Services

SERVICES SUB-SEGMENTS CAGR = 100-105%

Global system integrators (% contribution)	In-house services practices of ISVs (% contribution)
8-10%	**90-92%**

- Services remain limited to early proofs of concept with minimal solutions or service offerings
- The majority of services demand is likely to be fulfilled by in-house services practice of ISVs

SOFTWARE SUB-SEGMENTS CAGR = 90-95%

Cloud service providers (% contribution)	Enablement software ISVs (% contribution)
83-85%	**15-17%**

- The enablement software segment consists of technologies used to adopt and manage TEEs and TEE-based applications
- As the market matures, the contribution of enablement software is expected to rise
- Assumes a pricing premium of 1.5-2x regular compute for CSPs in 2021 with normalization over time

HARDWARE SUB-SEGMENTS CAGR = 100-105%

Silicon chipset OEMs (% contribution)	Assembled server OEMs (% contribution)
51-53%	**47-49%**

- Limited to no differential pricing in computing hardware for CC vs. regular will continue to drive the demand
- Contribution of silicon chipsets expected to outpace the assembled server market post 2024 owing to increased adoption in cloud environments

Why Confidential Computing?

Confidently Migrate to the Cloud, Knowing You're in Control

Even with confidential or regulated data

Collaborate with Multiple Parties on Beneficial Shared Analyses

While maintaining privacy & compliance

Strengthen Compliance & Data Sovereignty Programs

With technological controls

Harden Application Security & IP Protection

Hardware-based isolation and access controls

Why is Confidential Computing Essential for your Business?

Data Security and IP Protection

Protect apps and data from attack, tampering or theft

Privacy and Compliance

Strengthen data confidentiality and regulatory compliance

Data Sovereignty and Control

Prohibit access by cloud provider or other tenants; Add safeguards to data sovereignty & governance

Confidential Computing

Sectors & Use Cases

Sectors

Government

Financial Services

Retail

Healthcare

Industrial and Edge

Use Cases

Collaborative Analytics

Confidential AI

Privacy-preserving AdTech

Privacy-preserving Blockchains

Data and Software IP

Confidential Computing

Key AI Use Case

Multi-party machine learning

Leverage the power of machine learning without compromising the confidentiality and privacy of sensitive customer data

Business Brief

Multi-party machine learning with confidential computing can be especially useful in:

Healthcare

can leverage the power of data to conduct more advanced research without exposing confidential patient information

Financial Services

can better predict potentially fraudulent activities while also fighting money laundering and the financing of terrorism

Customer Case Study

Healthcare

Collaborative Computing with Regulated Data

BeeKeeperAI™ NOVARTIS

Situation

Novartis Biome develops diagnostic models and therapies for rare diseases. Rare disease information is sparse and dispersed across multiple hospitals and research institutions

Challenge

Patient information is private and highly regulated.
Hospitals do not want to move data off-prem or disclose private records to BeeKeeperAI or Novartis

Solution

An Intel® SGX-enabled BeeKeeperAI node installed onprem at each hospital analyzes private data and updates master model weights in the cloud. Neither Novartis nor BeeKeeperAI personnel ever see or store regulated health records

BeeKeeperAI™

"[Confidential computing platforms] allow us to reduce the cycle time to validate an algorithm in half. It also cuts the costs almost in half. Those kinds of savings allow us train, validate, and bring to market generalizable algorithms much faster. And, it will only get faster and less costly as the technology and processes underlying CCP mature." MaryBeth Chalk, Co-founder and Chief Commercial Officer, BeeKeeperAI, Inc

Whitepaper

Accelerating Development of Clinical AI Algorithms

Customer Case Study

High-Security Key Protection

Fortanix®

Situation

Rapidly proliferating keys and certificates require strong protection and centralized management. HSM solutions are expensive and cloud solutions rely on CSP security and compliance.

Challenge

Build a scalable, software-based key management system with HSM-like security that is technologically isolated from its cloud host

Solution

Fortanix bases its Self-Defending KMS software on Intel® SGX to protect keys and certificates from external adversaries and the cloud provider and helps ensure the owner's secrets remain under their control

Fortanix®

Performance Remains High with Intel® SGX Enabled

Implementing a multiple-instance configuration provides significant throughput gains. These performance enhancements are minimally affected by enabling Intel® SGX, meaning that organizations can simultaneously increase security and performance.

Solution Snapshot

[Confidential AI Data Intel Security Solution - Fortanix]

PRC Customer Case Study

Mining Data Value

创邻科技
CREATE LINK

Chuanglin Technology

Situation

How to ensure the security of enterprise data and privacy is a common problem faced by database and hardware manufacturers

Challenge

Traditional data encryption technology only encrypts hard disk storage and network transmission, and its effectiveness is based on the premise that the server control authority has not been leaked. If the control of the server is intercepted, the data in use can be stolen or modified by a third party

Solution

Chuanglin Technology and Intel jointly launched a graph database data encryption solution, using Intel® SGX memory encryption. It guarantees the ultimate performance of Galaxybase, thus creating a memory-safe graph database product.

创邻科技
CREATE LINK

It is believed that with the help of Intel® SGX memory encryption technology, the new-generation graph database Galaxybase created by Chuanglin Technology can provide customers with high-quality and more secure data services, efficiently realize data interconnection, and empower enterprises to realize the value of data assets in a stable manner.

Press Release

What Intel offers for Confidential Computing

4 Facts: Intel at the Foundation of Confidential Computing

2018 Intel® Software Guard Extensions (Intel® SGX) on Intel® Xeon® processors is the first Confidential Computing solution introduced into the data center

300+ Organizations have engaged with Intel to develop and deploy Confidential Computing services

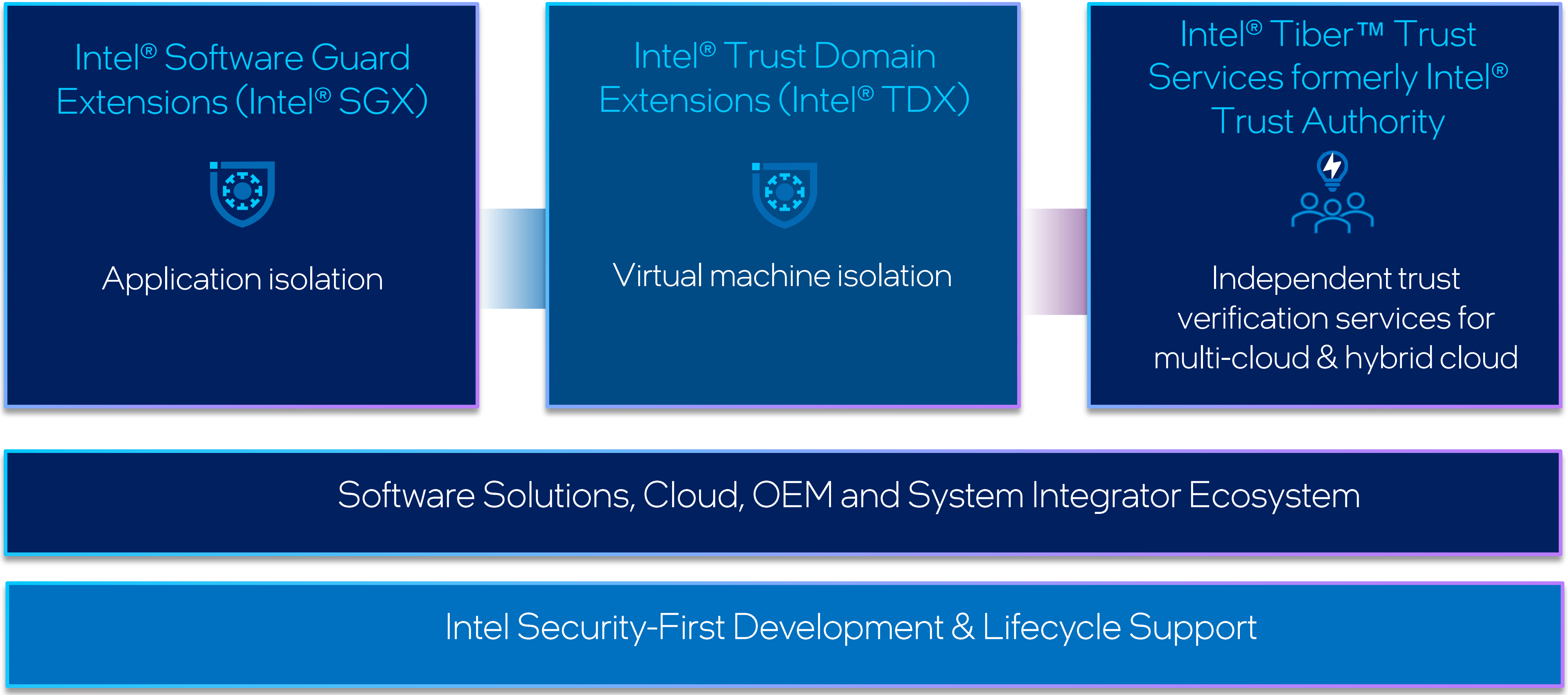
$300M Is the estimated value of infrastructure deployed with Intel® SGX on Intel® Xeon® processors

4 Global cloud providers have committed to offer Intel® Trust Domain Extensions (Intel® TDX) on 4th Gen Intel® Xeon® processors in 2023

Microsoft Azure IBM Cloud Google Cloud Alibaba Cloud

View video: Here

Intel Offers the Most Comprehensive Portfolio



Intel® Software Guard Extensions (Intel® SGX)

Application isolation

Intel® Trust Domain Extensions (Intel® TDX)

Virtual machine isolation

Intel® Tiber™ Trust Services formerly Intel® Trust Authority

Independent trust verification services for multi-cloud & hybrid cloud

Software Solutions, Cloud, OEM and System Integrator Ecosystem

Intel Security-First Development & Lifecycle Support

*Intel® TDX available through select cloud providers

Intel® Tiber™ Trust Services

formerly Intel® Trust Authority

Put Zero Trust Within Reach and Get Public Cloud Flexibility with Private Cloud Security

Intel® Tiber™ Trust Services is a new portfolio of software and services that brings enhanced security and assurance to Confidential Computing with Zero Trust principles

In its first generation, it offers an independent attestation service that attests to Trusted Execution Environments (TEEs) that are based on (Intel® SGX) and (Intel® TDX)

Implement the tenets of Zero Trust without incurring the cost and complexity of building your own attestation service

Independent → Scalable → Easy to Deploy

Learn More

Product Brief

What That Means Video

Noname Case Study

noname

Thales Case Study

THALES

Zscaler Case Study

zscaler

Confidential Computing

Software & Solution Ecosystem for Intel® SGX

Commercially Supported Solutions → Build It Yourself

Commercial Solution Providers

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

Curated, Ready-to-Deploy Containers (through Q1'23)*

PyTorch, redis, scikit learn, Spark, TensorFlow

Developer Tools

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

Systems Integrators

accenture, KPMG, Capgemini, IBM, Atos, leidos, avanade

Hypervisors (SGX)

KVM 5.13 & later, vmware vSphere 8

* Available at Azure Marketplace

Intel® TDX Availability

Intel® TDX is available on 4th Gen Intel® Xeon® Scalable instances in public preview through three leading cloud providers

Click on the logos below for more information on each cloud provider's offering

Microsoft Azure

Alibaba Cloud

Google Cloud

IBM Cloud
*public preview TBA

Intel® TDX is enabled on the following guest OS vendors

Red Hat

SUSE

Canonical Ubuntu

*Intel® TDX becomes generally available with 5th Gen Intel® Xeon® Scalable processor in 2024

Competitive Comparison

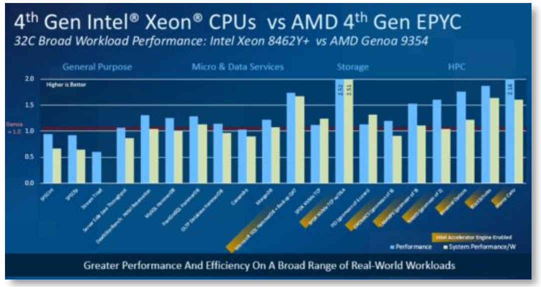
	Intel® SGX	Intel® TDX	AMD SEV-SNP	AWS Nitro Enclaves	Conf. Comp on Nvidia H100 GPU
Cloud infrastructure provider's hardware/firmware, hypervisor and cloud management stack excluded from trust boundary	●	●	●		●
Available through multiple cloud providers to facilitate multi-sourcing	●	● [1]	●		●
Designed to accommodate legacy applications with low or no porting, re-design or re-packaging		●	●		◉ [2]
Attestation of hardware authenticity & correct TEE launch	●	●	●	●	●
Attestation of integrity of software image loaded in TEE	●	◉ [3]	◉ [3]	●	
Confidential data only accessible by designated application code; VM admin, Guest OS, other apps and cloud stack excluded from access	●				
Deployable on "bare metal" servers without virtualization	●				●
Hardware-based, cryptographic memory integrity option for additional Rowhammer protection	●				
Compatible with Intel® Tiber™ Trust Services	●	●			
Competitive Data Sources as of March 2023			Link, Link	Link, Link, Link	Link

[1] Intel® TDX instances coming online at select cloud providers in 2023; Availability timing will vary

[2] No or low changes for legacy code running on GPU. Portions of the workload that use the CPU would need to incorporate a CPU-based TEE and a means of protecting PCIe communications.

[3] Not an inherent capability of available hardware technology but is feasible as value-added capability delivered by the cloud or attestation service provider.

4th Gen Intel® Xeon® Competitive Analysis



4th Gen Intel® Xeon® CPUs vs AMD 4th Gen EPYC

32C Broad Workload Performance: Intel Xeon 8462Y+ vs AMD Genoa 9354

Greater Performance And Efficiency On A Broad Range of Real-World Workloads

4th Gen Intel® Xeon® Scalable processors outperforms competition on Real-World Workloads

intel XEON vs EPYC AMD

4th Gen Intel® Xeon® Scalable processors on software optimized for CPUs perform up to 2.5x faster than NVIDIA A100 GPUs

intel XEON vs NVIDIA

Leadership Data Center Performance with 4th Gen Intel® Xeon® Scalable processors

intel XEON vs EPYC AMD

Why Choose Intel for Confidential Computing?

Why Choose Intel for Confidential Computing?

Technology Options to Meet Diverse Security Needs

Only Intel offers both app isolation (Intel® SGX) and VM isolation (Intel® TDX) so customers can precisely tune solution for varying levels of security

Broad Solution Ecosystem

Intel partners with dozens of ISVs and cloud providers to offer hosting services & software solutions, including Confidential AI, analytics, blockchain, databases and more

Access to Experts at Intel and our Solution Partners

Intel experts are ready to assist customers with solution architecture, partner matching, POC resources and deployment troubleshooting

Connect with your Intel Representative for more info

How Intel® Partner Alliance can help

Get Started with Intel® Partner Alliance

Intel Partner Alliance membership gives you exclusive business-building opportunities, like entry to our global marketplace, advanced training, and promotional support – all tailored to your needs

Training and Competencies

Admission to Intel® Partner University provides you with specialized training on advanced technologies, competency programs and rewards for learning

Marketing Resources

Entry to the Intel® Solutions Marketplace and the Intel® Marketing Studio helps you create more demand for your products and services

Valuable Rewards

Earn points for your qualifying activities, advance your membership status and get access to additional resources to build your business

If you're not already a Member

Join Now

Benefits of a Membership

Earn Points

One of the most popular and differentiated benefits within Intel® Partner Alliance are points we award partners to recognize their business results with Intel and their engagement in high priority activities.

There are over 1,000 ways to earn points within Intel Partner Alliance, and 100's of redemption opportunities.

Cloud Insider Community

Intel® Cloud Insider Community offers continuously refreshed, world-class cloud content and tools. Members have the opportunity to connect with peers and the ecosystem to take innovative, joint cloud solutions to market

Learn More

Industry Insights

Gold and Titanium members can access specifically curated quarterly industry insights to help fuel their growth

Learn More

Financial Incentives

Membership unlocks powerful marketing development funds and incentive programs to accelerate your product marketing success

Speak to your Intel Representative to learn about Intel Partner Alliance Accelerator Initiatives and more Financial Incentives

How to Access Intel® Partner Alliance Customer Support

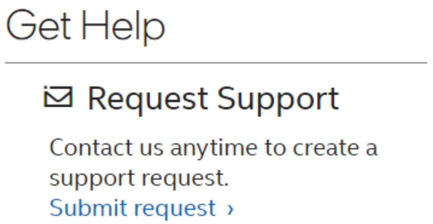
Intel Virtual Assistant

This Chat Bot, located in the bottom-right corner of each Partner Alliance webpage, provides self-help to most questions or a quick link to a live support agent.

Get Help "Blade"

Submit an online support request.

This link is found on the footer of most pages within the Partner Alliance website.



Get Help

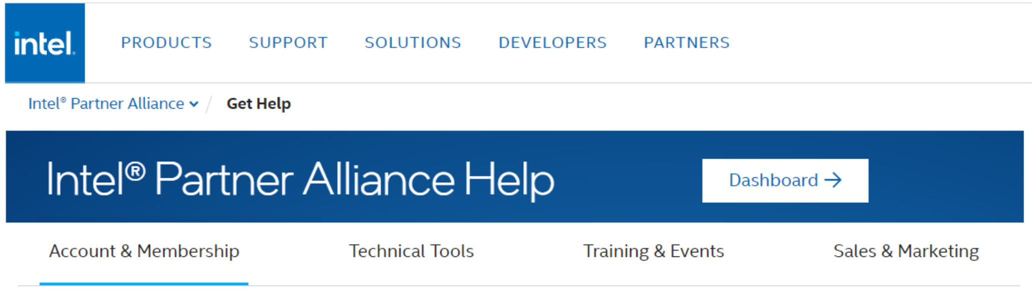
✉ Request Support

Contact us anytime to create a support request.

Submit request ›

Partner Alliance "Get Help" page

The Get Help page provides detailed self-help guides on most of the tools and benefits available to Partner Alliance members.



intel. PRODUCTS SUPPORT SOLUTIONS DEVELOPERS PARTNERS

Intel® Partner Alliance ⌄ / Get Help

Intel® Partner Alliance Help

Dashboard →

Account & Membership | Technical Tools | Training & Events | Sales & Marketing

Resources

Cloud TV

Intel® Cloud TV explores cloud computing news, trends, and strategies to drive your success

Sapphire Rapids in the Cloud

Learn How to Protect Your Cloud Assets

Security in the Cloud

Security Challenges in the Cloud

Confidential Computing
Information and Resources

30-3-30

Confidential Computing 30-3-30

Videos

Confidential Computing Overview

Security is a challenge

Infographic

How to Defeat Cloud Security Threats

Research Paper

Protecting Data and Models within Emerging AI Workflows

Tech Articles

The State of Confidential Computing

An Introduction to Cloud Security

Blogs

A New Paradigm of Performance & Cybersecurity

Security Begins with Intel

intel

Additional Resources

Performance Index

4th Generation Intel® Xeon® Scalable Processors

Live Webinars

Cloud Solution Architect (CSA) Tech Talk: Reduce TCO and Improve Efficiency with 4th Gen Intel® Xeon® Scalable Processors

Recorded Webinars

Cloud Solution Architect (CSA) Tech Talk: Accelerating Critical Workloads with 4th Generation Intel® Xeon® Scalable Processors

Additional Training

Competencies and Certifications

Confidential Computing
Training Links

Security Training Links

Courses / Training

Topic -- Audience
3 Key Technologies to Grow Your Cyber Security Resilience DevOps, Cloud Architects – Confidential Computing
End to End Security for IOT Solutions DevOps
Edge to Cloud Security DevOps, Cloud Architects
Virtual Private Cloud, Cloud Networking and Cloud Security DevOps
Security Value in Intel® Products and Solutions ALL
Securing Applications in the Cloud DevOps
Security in Cloud Computing DevOps, Cloud Architects

Topic - Audience
Virtual Private Cloud, Cloud Networking and Cloud Security DevOps, Cloud Architects
Security in the Business Conversation Cloud Architects, C-Suite
An Encryption Primer for Intel Architecture DevOps
Security Value in Intel® Products and Solutions DevOps, Cloud Architects

intel®

Backup