August 2024

Confidential Computing SI and Reseller Enablement Package

How System Integrators and Resellers can address customers' business challenges with Intel based solutions

intel

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
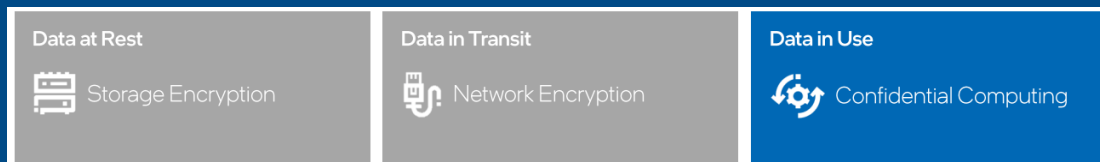
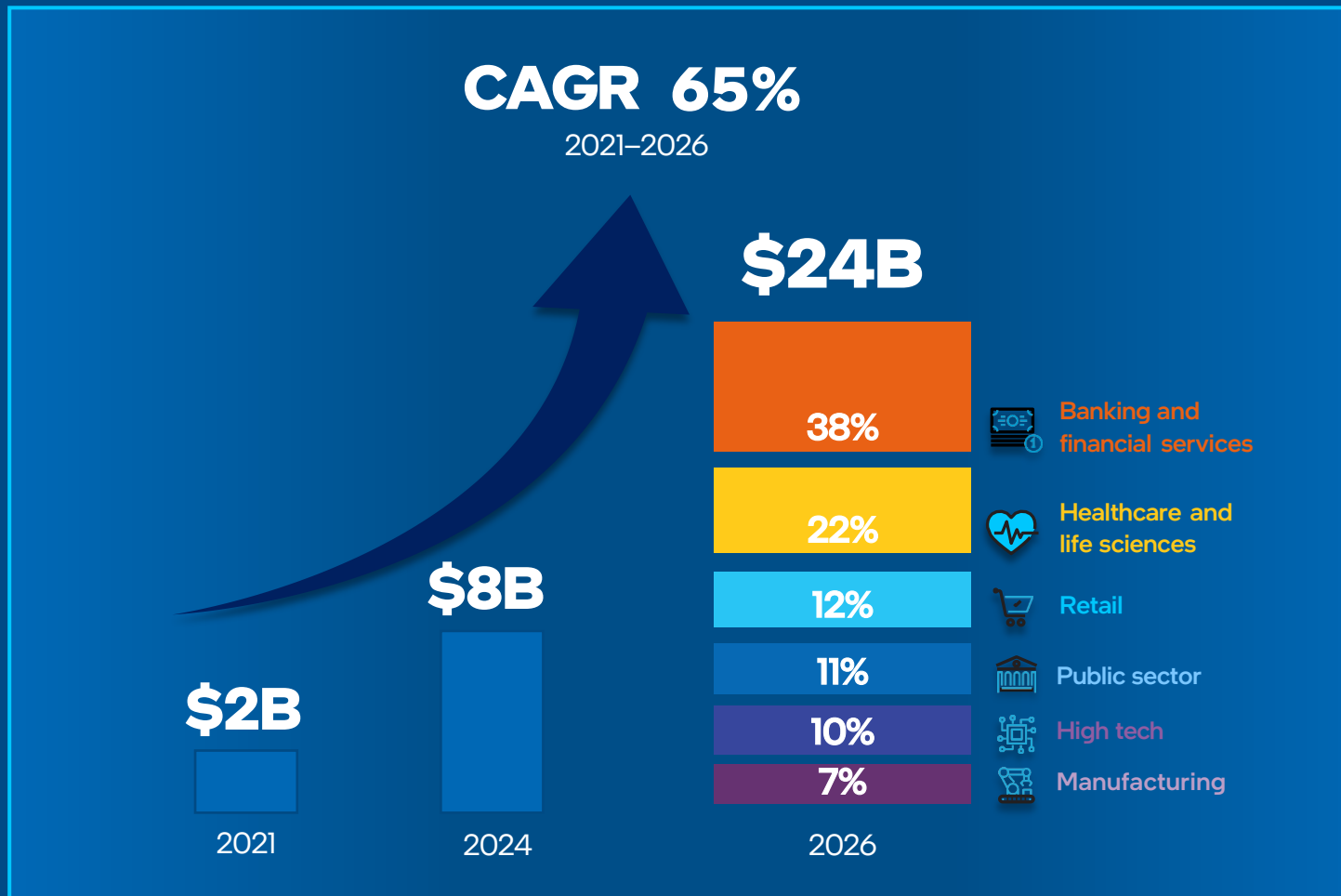READ MORE > **Essentials of Confidential Computing**

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.
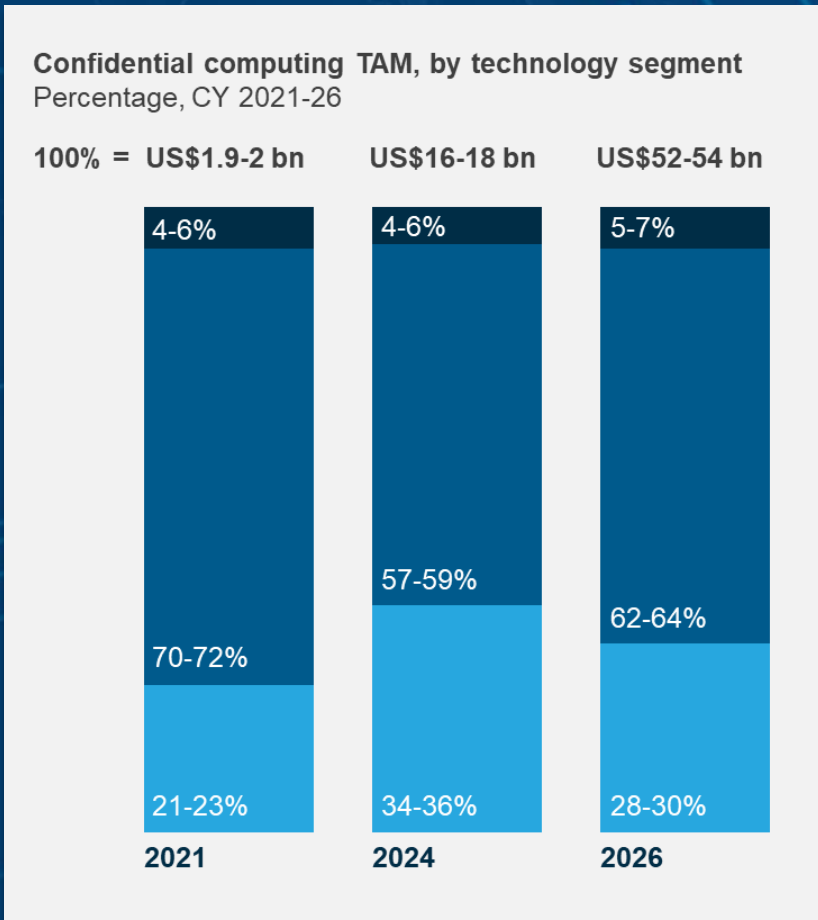
intel

Confidential Computing Market Forecast

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

CAGR 65%

2021–2026

$24B

38%	Banking and financial services
22%	Healthcare and life sciences
12%	Retail
11%	Public sector
10%	High tech
7%	Manufacturing

$8B

$2B

2021   2024   2026

intel.

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

100% =	US$1.9-2 bn	US$16-18 bn	US$52-54 bn
Services	4-6%	4-6%	5-7%
Software	70-72%	57-59%	62-64%
Hardware	21-23%	34-36%	28-30%
	2021	2024	2026

Legend: ■ 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

Confidential Computing Outcomes

Migrate to the Cloud & Activate Data Knowing You're in Control

Even with confidential or regulated data

RBC Bank / Microsoft Azure

Collaborate with Multiple Parties on Beneficial Shared Analyses

While maintaining privacy & compliance

Novartis / BeeKeeperAI

Strengthen Compliance & Data Sovereignty Programs

With technological safeguards

Deutsche Telekom Sovereign Cloud

Harden Application Security & IP Protection

Hardware-based isolation & access controls

"Social Media & Advertising Giant"

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 Landscape is Evolving Rapidly

Confidential Computing ▶ **Confidential Computing inclusive of Confidential AI**

Confidential AI Maps Directly to Regulations Affecting Customers

Capabilities

- ☑ Helps prevent data exposure to unauthorized software or persons

- ☑ Protects AI training or inference data from exposure or manipulation

- ☑ Protects the AI model from tampering or theft inside an attested TEE

- ☑ Strengthens cybersecurity against known and new threats such as unpatched or Zero Day vulnerabilities and malicious insiders

intel.

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

READ MORE

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

Business Brief
4th Gen Intel® Xeon® Scalable Processor
AI and Machine Learning

Advance Insights with Artificial Intelligence

intel

With Intel you can get better insights for critical business outcomes.

Taking AI from concept to production at scale has been a challenge. Advanced AI models once required specialized hardware, advanced skills and custom tools to turn data into business results. Making AI work across the entire end-to-end pipeline — whether on premises, in the cloud or using a hybrid approach — often meant additional expense coupled with difficulty recruiting the right talent. For business leaders struggling with how to scale AI across their businesses, reducing complexity is key.

It's now more critical than ever for technology to deliver business value as organizations look to scale, drive down costs and deliver new services. Instead of customizing systems for new applications, which adds yet another layer of complexity, enterprises can achieve the performance they need to meet a wide variety of deployments — both today and in the future — with a scalable platform.

| 84% BELIEVE THEY NEED AI TO SUCCEED | 70% RUNS ON INTEL® XEON® PROCESSORS | 90% OF ENTERPRISE APPS WILL USE EMBEDDED AI |

Accelerate your AI with Intel technologies

4th Gen Intel® Xeon® Scalable processors have the most built-in accelerators of any CPU on the market to deliver performance and power efficiency advantages across the fastest-growing workload types in AI, analytics, networking, storage and HPC. With all-new Intel Advanced Matrix Extensions (Intel AMX), 4th Gen Intel Xeon Scalable processors have exceptional AI training and inference performance. To enable new built-in accelerator features, Intel supports the ecosystem with OS-level software, libraries and APIs.

With built-in accelerators and software optimizations, previous generation Intel® Xeon® Scalable processors have been shown to deliver leading performance per watt on targeted real-world workloads. This results in more efficient CPU utilization, lower electricity consumption, and higher ROI, while helping businesses achieve their sustainability goals.

PERFORMANCE PROOFPOINT

5.7X TO 10X HIGHER PYTORCH REAL-TIME INFERENCE PERFORMANCE   3.5X TO 10X HIGHER PYTORCH TRAINING PERFORMANCE

with built-in Intel AMX (BF16) versus the prior generation (FP32)

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

READ MORE

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**

Accelerating Development of Clinical AI Algorithms CASE STUDY

At a Glance:
- BeeKeeperAI provides a secure way for algorithm owners to compute on the real-world data they need to achieve generalizability while the data remains in control of the data steward at the originating institution.
- BeeKeeperAI has worked to validate three different clinical models using an Intel® technology-based confidential computing platform, including a hemodynamic stability index, a COVID-19 detection tool, and a treatment stratification tool for diabetic retinopathy.

Download the one-page summary

Customer Case Study - PRC

Financial Services
Software-as-a-Service Solution

ANT GROUP

Situation

Ant Group is developing LLMs to power new financial solutions in China. These include intelligent assistants for both consumers and industry professionals.
End customers can even use their data to fine-tune the LLMs, enhancing the value of their assistants.

Challenge

Ant Group is exploring various ways to allow customers to fine-tune its LLMs with their own data, however, they must ensure to:
- Maintain the confidentiality of proprietary and customer data
- Protect intellectual property (IP)
- Strengthen compliance with regulations

Solution

On Alibaba Cloud Elastic Compute Service (ECS) g8i instances, Ant Group built a confidential platform-as-a-service (PaaS) product matrix. The company used 4th Gen Intel® Xeon® Scalable processors with Intel® Trust Domain Extensions (Intel® TDX), a hardware-based trusted execution environment (TEE) that helps secure customer data and Ant Group AI models while in use.

ONE PAGER

ANT GROUP

"Ant Group has built a complete confidential PaaS (Platform as a Service) product matrix on Alibaba Cloud ECS instances: the confidential computing engine Occlum and the confidential computing service KubeTEE. Based on this confidential PaaS, Ant Group also offers confidential SaaS solutions for financial scenarios, such as the Ant Privacy-Enhancing Data Analytics Platform, Ant PrivacyEnhancing AI Platform, and more." **— Shuang Liu, Ant Group, Confidential Computing Team Lead**

READ MORE

Ant Group Develops Confidential Computing for Financial SaaS Solutions with Intel Technologies
CASE STUDY

intel XEON
Case Study
Confidential AI
Intel® Trust Domain Extensions (Intel® TDX)
Ant Group Develops Confidential Computing for Financial SaaS Solutions with Intel Technologies

intel®

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.

READ MORE > Strengthen data security while unlocking new value with confidential computing solutions

READ MORE

Solution Design Brief

Solution Design Brief
Data Centers | Confidential Computing
Intel Accelerated Solution

intel.

Securely Use Confidential Data with Intel® Software Guard Extensions and Fortanix Confidential AI

Business Challenge: How do you safeguard sensitive data, valuable intellectual property and competitive insights without slowing AI performance or creating data silos?

Enabling Sovereign Landing Zones with Confidential Computing

Confidential Computing with Intel® Xeon® Scalable processors

Intel's broad portfolio of Confidential Computing technologies allows organizations to choose the level of security they need to help meet their business needs and regulatory requirements

Intel is the only company that offers Confidential Computing solutions at both the application and the VM level

intel accenture > SCONE

The power of Intel, Accenture, Scone, and cloud service providers enables:

- Business transformations – design of fit-for-purpose solutions by the COEs

- Enhanced confidentiality, integrity, consistency, scalability, and resiliency

- Extremely secure instantiations of landing zones, including Scone CAS and security guardrails

- Automating the deployment pipeline to land workloads in their respective landing zone

READ MORE

Enabling Sovereign Landing Zones with Confidential Computing White Paper

intel

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

Intel Offers the Most Comprehensive Security Portfolio for Confidential Computing

Confidential computing with trusted execution environments (TEEs) helps protect data and AI models

With 4th and 5th Gen Intel® Xeon® processors, you can choose from the most researched and updated confidential computing options in data centers on the market today

READ MORE

Intel® Software Guard Extensions (Intel® SGX)

Application isolation

Intel® Trust Domain Extensions (Intel® TDX)

Virtual machine isolation

*Intel® TDX available through select cloud providers

Intel® Tiber™ Trust Services formerly Intel® Trust Authority

Independent trust verification services for multi-cloud & hybrid cloud

PERFORMANCE PROOFPOINT

Up to

4x higher VPP IPSec (1420B) throughput[1]

with the new 5th Gen Intel Xeon Platinum 8592+ processor compared to the 3rd Gen Intel Xeon Processor

Confidential Computing 1-pager

[1]See [N13] at intel.com/processorclaims: 5th Gen Intel Xeon processors. Results may vary

intel 16

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

Product Brief

Independent Attestation by Intel® Trust Authority

intel

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

Video

CASE STUDIES
click on logos for more info

noname   zscaler   THALES

Intel® TDX Availability

Intel® TDX is available on 4th and 5th 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

5th gen Intel® Xeon®

WHITE PAPER >   Alibaba Cloud ApsaraDB Confidential Database Empowered By Intel® TDX

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.

Intel Strength in Product Security Assurance

Peace of Mind

ABI Research ranked
Intel #1 in Security Assurance based
on design practices, proactive
research and security support.[1]

Intel® TDX underwent more than a
year of intense security evaluation by
Google, Microsoft and 18 elite ethical
hackers, with all findings addressed.[1]

**In 2023, AMD reported 2.5x as
many vulnerabilities in their
Confidential Computing
firmware components and
features than Intel.[1]**

Why Choose Intel for Confidential Computing?

intel.

Why Choose Intel for Confidential Computing?

Technology Options to Meet Diverse Security Needs

Intel **leads the silicon industry** in product security assurance[1]

Only Intel offers app isolation (Intel® SGX), VM isolation (Intel® TDX), and independent attestation (Intel® Tiber™ Trust Services) so customers can tune their solution to meet business requirements

Broad Ecosystem Deployment

Over **300** organizations have engaged with Intel + **80** ISVs enabled on Intel platforms to develop and deploy Confidential Computing services around the world[2]

Access to Experts at Intel and Solution Partners

Intel partners with dozens of ISVs and cloud providers to offer hosting services & software solutions, including cutting-edge work on Confidential AI
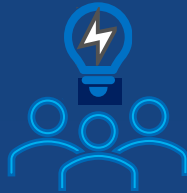
Intel experts are ready to assist customers with solution architecture, partner matching, POC resources, and deployment troubleshooting

[1]https://www.intel.com/content/www/us/en/security/security-as-a-component-of-tech.html
[2]https://www.intel.com/content/www/us/en/content-details/781567/four-facts-intel-at-the-foundation-of-confidential-computing.html

Next Steps

Collaboration

Learn more about Confidential Computing and how working with Intel can produce successful outcomes.

Confidential AI exists at the intersection of AI and confidential computing, designed to secure private data and AI models.
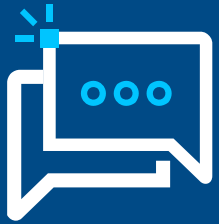
Connect

Get Started Today

Connect with your Intel representative to understand more about Intel Confidential Computing Technical Portfolio in the ecosystem

Resources

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.

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.

Cloud TV

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

How Intel® Trust Authority Enhances Security

How Confidential Computing Enhances Security

Security Challenges in the Cloud

Confidential Computing
Information and Resources

intel

30-3-30

- Confidential Computing 30-3-30
- Data Protection, Compliance & Sovereignty with Intel Confidential Computing (Non-Public)

Videos

- Confidential Computing Overview
- Security is a challenge

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

Infographic

- How to Defeat Cloud Security Threats

Additional Resources

- [Confidential AI at Intel](#)

- [Intel® Confidential Computing Solutions](#)

- [Intel® Software Guard Extensions (Intel® SGX)](#)

- [Intel® Trust Domain Extensions (Intel® TDX)](#)

Training

Confidential Computing 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