August 2024

Confidential Computing ISV Enablement Package

How ISVs 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

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.

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

Confidential AI

Use Case Example

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

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

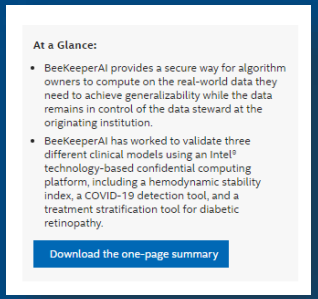
An Intel® SGX-enabled BeeKeeperAI node installed onprem at each hospital analyzes private data and updates master model weights in the cloud. Neither Novartis nor BeeKeeperAI personnel ever see or store regulated health records

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**

READ MORE

Accelerating Development of Clinical AI Algorithms
CASE STUDY



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.

ANT GROUP

ONE PAGER

"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

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

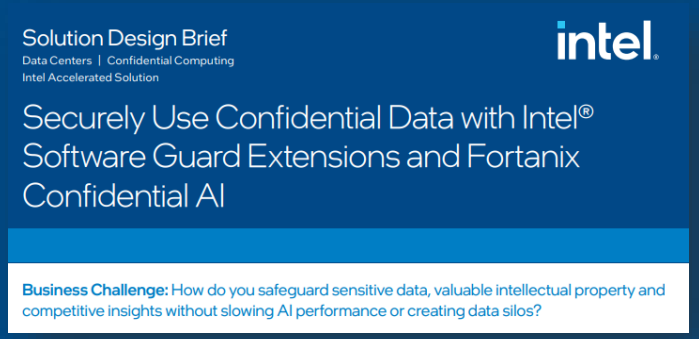
Fortanix®

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



What Intel offers for Confidential Computing

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 Trusted Execution Environments

Application-level isolation: **Intel® SGX**

Advantages

- Separation from cloud provider and other tenants
- Smaller trust boundary and potential attack surface
- More amenable to code inspection and monitoring
- Deployable in VMs, cloud-native containers and bare-metal

Considerations

- Apps may require specific development or tailoring
- Frequent calls outside the enclave may impact performance

SOLUTION BRIEF

Microsoft moves credit card transactions to Azure Cloud Services running Intel® Software Guard Extensions (Intel® SGX)

Microsoft

VM-level isolation: **Intel® TDX**

Advantages

- Separation from cloud provider and other tenants
- Lowest porting effort for existing applications
- More amenable to enterprise-wide deployment mandates
- Can be a simple instance configurator setting

Considerations

- Larger trust boundary (guest OS, all apps, VM admins)
- Possible re-validation with updated guest OS & hypervisor
- Less granular attestation

INFOGRAPHIC

READ MORE

Which Intel Trusted Execution Environment is right for you?

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

Video

CASE STUDIES

click on logos for more info

noname zscaler THALES

Intel® Tiber™ Trust Services

formerly Intel® Trust Authority

Get Started with Intel® Tiber™ Trust Services

How It Works

1

Set up or request from your cloud infrastructure provider a confidential computing environment (TEE) instance based on Intel® SGX for workloads or Intel® TDX for virtual machines (VMs)

2

- Identify and enable workloads to run in these confidential computing environments
- This can be done at an application level with Intel® SGX (facilitated by Gramine or another client library) or at a VM level with Intel® TDX

3

- Subscribe to get an Intel® Trust Authority attestation key
- Insert the key into the client library on the workload (Intel® SGX) or VM (Intel® TDX) so it can communicate directly with the SaaS to verify the TEE

Learn more about Intel® Tiber™ Trust Services

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

How to Get Started

Intel® Software Guard Extensions (Intel® SGX)

More information Get Started

Cloud Service Providers

Click on logos for more info

Azure CORE OVHcloud phoenixNAP swisscom IBM Cloud CloudSigma

OEMs

Click on logos for more info

Hewlett Packard Enterprise SUPERMICRO

Training & Documentation

Training Videos Technical Library Solution Brief

Intel® Trust Domain Extensions (Intel® TDX)

More information

Documentation

Trust Domain Security Guidance for Developers

Get Started

Intel® Trust Domain Extension (Intel® TDX) Module Download Beta

Intel® Trust Domain Extension (Intel® TDX) Loader

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]

[1]Source: 2023 Intel Product Security Report

Why Choose Intel for Confidential Computing?

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

Cloud Solutions Architect Certification

Completion of the CSA curriculum equips you with expert-level knowledge of cloud instance details, topics, and solutions

This curriculum is optimized for cloud solution architects with at least two years of experience implementing solutions in the cloud

What You'll Gain

Improve your knowledge and skills related to cloud technologies and solutions architecture to augment the design and implementation of cloud solutions.
Enhance your understanding of the latest industry trends, delivered through interactive courses and lessons designed for online—this makes it simple for learners to advance at their own pace and minimize interruptions to their work and personal time.
Gain advanced knowledge from hands-on labs and deep dives into advanced cloud applications, across a wide variety of cloud workloads, from container orchestration, AI workloads, and instance tuning through the cloud-based CI/CD pipeline.
Obtain industry-recognized certification and credentials based on a hosted/proctored exam.

Start Your Self-Paced Online Certification Training Now

Confidential Computing
Information and Resources

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

Confidential Computing
Resources for DevOps & Cloud Architects

Tech Papers

- Accelerated AI Inference with Confidential Computing
- Accelerate innovation and enhance data protection with Intel® Security Engines

White Paper

- How to Defeat Cloud Security Threats
- Enabling Sovereign Landing Zones with Confidential Computing

Newsletter

- Intel Developer Zone Newsletter

Communities

- Intel Community
- Security Community Partners

Videos

- Intel Security Accelerators Video

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


intel