Everest Group®

Confidential Computing – The Next Frontier in Data Security

October 2021

CONFIDENTIAL COMPUTING CONSORTIUM

Contents

For more information on this and other research published by Everest Group, please contact us:

Ronak Doshi, Partner

Abhishek Mundra, Practice Director

Arjun Chauhan, Senior Analyst

Suseel Menon, Senior Analyst

01

Introduction

- Report sponsorship
- Key objectives
- Sources leveraged

This research was paid for, in part, by the Confidential Computing Consortium

The Confidential Computing Consortium is a project community at the Linux Foundation focused on projects securing data in use and accelerating the adoption of confidential computing through open collaboration

Premier Members

accenture, 蚂蚁集团 ANT GROUP, arm, facebook, Google, HUAWEI, intel, Microsoft, Red Hat

General Members

AMD, AMPERE, anjuna, Anqlave, appliedblockchain, ByteDance, cisco, cosmian, CRUST, CYSEC, DECENTRIQ, EDGELESS SYSTEMS, ENVEIL, Ethernity CLOUD, Fortanix, iExec, MADANA, NVIDIA, PHALA NETWORK, Profian, r3, swisscom, vmware, Western Digital, XILINX

Key objectives

Although adoption of confidential computing is nascent, its potential is tremendous, not only for the enterprises that are consuming it but also for the technology and service providers that are enabling it.

In this study, we analyze the confidential computing market with the following two objectives in mind:

1

To ascertain the scope and size of the confidential computing market globally

2

To create market insights on key trends and perspectives on use cases for confidential computing

Scope of the market assessment

Geography
Global

Industry
Cross-industry

Technology
- Services
- Software
- Hardware

Use case
Cross-use case

Information sources | we used multiple sources of data to assess the confidential computing market

Proprietary datasets
Everest Group's used its published research across technology segments and our service provider and product vendor database of 300+ providers.

Primary consultations with key market stakeholders
Everest Group engaged key stakeholders across the confidential computing, cybersecurity, and cloud technology domains to gain a holistic perspective of enterprise requirements and to identify market movements.

Contributions from members of the Confidential Computing Consortium (CCC)
Everest Group collated RFI data from participating CCC members to analyze the market opportunity presented by confidential computing and interviewed senior stakeholders within participating member organizations to develop a deeper qualitative analysis of the market.

Confidential Computing Consortium members that contributed to this report include:

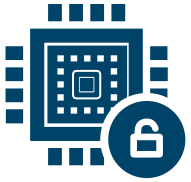
accenture · anjuna · 蚂蚁集团 ANT GROUP · arm · DECENTRIQ · Fortanix · intel · Microsoft · r3.

02

Overview of confidential computing

- Importance of confidential computing
- Everest group's definition of confidential computing

Confidential computing provides end-to-end data protection across the rest, transit, and in use phases



Protection at rest	Protection in transit	Protection in use
Securing data being stored by encrypting it before storing it or encrypting the device itself	Securing data transmitted between networks using end-to-end encryption or by using encrypted connections	Protecting data by encrypting it while it is being used in the RAM or processor for computation

Prevalent data security model

Current security models adequately mitigate risks involved with storage and transmission of data but fail to address risks of exposing data while its being processed

Holistic data security model

Emerging security models encourage the adoption of a comprehensive protection model that mitigates risks across the data lifecycle from transmission to storage and usage, which can be achieved through confidential computing

Confidential computing helps build a resilient and secure enterprise by ensuring data integrity and confidentiality, and code integrity

Confidential computing is a privacy-preserving computation principle that leverages hardware-based Trusted Execution Environments (TEE) to protect data being processed.
A TEE is a secure area within a main processor that runs an isolated environment parallel to the main operating system. Through this hardware-level isolation, the TEE guarantees that data and code uploaded into it cannot be tampered with by malicious agents.

Key characteristics of confidential computing[1]

Data confidentiality
Unauthorized entities cannot view data while it is in use within the TEE

Data integrity
Unauthorized entities cannot add, remove, or alter data while it is in use within the TEE

Code integrity
Unauthorized entities cannot add, remove, or alter code executing in the TEE

1 As defined by the Confidential Computing Consortium; for additional information please visit: confidentialcomputing.io/white-papers

Market segments | Everest Group's definition of confidential computing market segments

HARDWARE

Hardware and hardware architectures that help create isolated, non-virtual environments for secure execution of code and data

- Hardware architectures for Trusted Execution Environment (TEE)
- Microprocessors and microcontrollers
- TEE-based HSM devices
- TEE-capable servers
- Trusted platform modules

SOFTWARE

Software used to operate hardware-based trusted execution environments

- Hypervisors and operating systems for TEE
- Infrastructure-as-a-service such as TEE-based VMs and containers from cloud hyperscalers including AWS, Azure, GCP
- Hardware and software attestation services
- Platform licenses and platform-as-a-service
- Homomorphic encryption

SERVICES

Implementation, integration, and managed services for building or migrating applications to a hardware-based TEE

- Application development services
- Integration services for confidential computing applications
- Managed services for confidential computing applications
- Software and hardware engineering services

Market segments | description of confidential computing market segments

Exclusions

Classification	Components	Description
Hardware	Hardware architectures for TEE	Licensing of semiconductor designs/architectures that enable creation of hardware for TEEs
	Microprocessors and microcontrollers	Silicon-based processing devices designed to support the creation of TEEs
	TEE-based HSM devices	Devices that can replicate the functions of an HSM using TEEs
	TEE-capable servers	Pre-assembled server packages running TEE-capable hardware
	Trusted Platform Modules	Silicon devices that can securely store artifacts used to authenticate platforms
Software	Hypervisors and operating systems for TEE	Virtualization and operational software required for creating TEE on compatible hardware
	Infrastructure-as-a-service such as TEE-based VMs and containers	Cloud computing service that provides TEE-based compute to run applications
	Attestation services	Software service that helps applications verify the integrity of the hardware used in TEE
	Platform licenses and platform-as-a-service	Software platforms that provide components and services that aid in the creation and management of TEE-based applications
	Homomorphic encryption	Software technique that permits performing computations on encrypted data without decryption
Services	Application development services	Third-party services to develop applications that utilize TEE
	Integration services for confidential applications	Application and middleware integration services for TEE-based applications
	Managed services for confidential applications	Third-party services for management and maintenance of TEE-based applications
	Software and hardware engineering services	Outsourcing engineering and development of TEE-based software products by ISVs

03

Market potential overview

- Executive summary
- Market opportunity by segment
- Industry and geography distribution of market opportunity
- Scenario analysis of the total addressable market

Executive summary of key findings | confidential computing market opportunity

The CC market is poised for exponential growth

- The Total Addressable Market (TAM) for confidential computing in 2021 is **US$ 1.9-2.0 billion**
- The CC market is expected to grow at a **CAGR of 90-95%** in the best-case scenario and **40-45%** in the worst-case scenario through 2026
- Cyber risks, regulations, and avenues for incremental revenue position CC for hyper growth

The hardware and software segments drive adoption

- The CC software segment, driven particularly by cloud service providers, is likely to constitute **~60-70% of the TAM** between 2021 and 2026
- The CC hardware segment is expected to approximately **double every year** through 2026
- Contribution of services segments will grow marginally over the next five years

Regulated industries will dominate roll-out

- **Over 75%** of demand is driven by regulated industries like banking, finance, insurance, healthcare, life sciences, public sector, and defense in 2021
- Awareness of the benefits of CC and willingness to invest in exploration is expected to **double across key regulated industries** through 2026

Enterprises in NA and Asia have the largest appetite

Adoption varies by geography because of privacy regulations and incidence of cyber threats

- North America is expected to constitute ~40% of the overall TAM
- APAC (ex-China) will be ~20-25% of TAM with China independently accounting for ~10-15%
- Europe accounts for about 25% of TAM given its robust regulatory frameworks

Key use cases reduce privacy and security risks

- **Privacy and security** use cases, particularly on public cloud, have gained the largest traction accounting for **30-35% of overall TAM**
- Emerging technologies such as **multi-party computing and blockchain** account for a large share of the market given how CC enhances the value delivered by these technologies

Considerations for executives

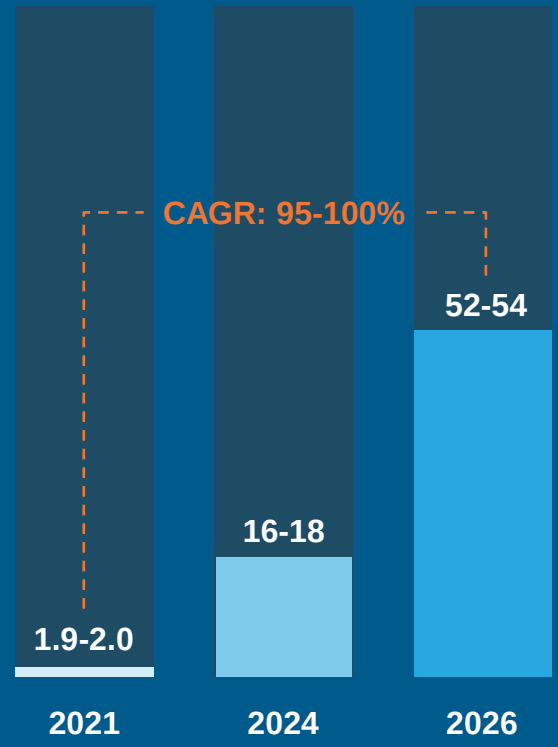
1. Given the wide applicability of confidential computing, enterprises must begin experimenting to understand potential areas of adoption
2. Early exploration will determine the amount of hardware control required and subsequent talent needs
3. CC has the potential to become a standard for end-to-end security; enterprises must plan to begin scaling proofs of concept in three to five years
4. It is imperative for suppliers to drive ecosystem growth and new use case exploration
5. Confidential computing's wide security implications and enablement of disruptive technologies creates a golden growth opportunity

The confidential computing market is likely to grow exponentially over the next few years, driven by enterprise cloud and security initiatives

Key takeaways

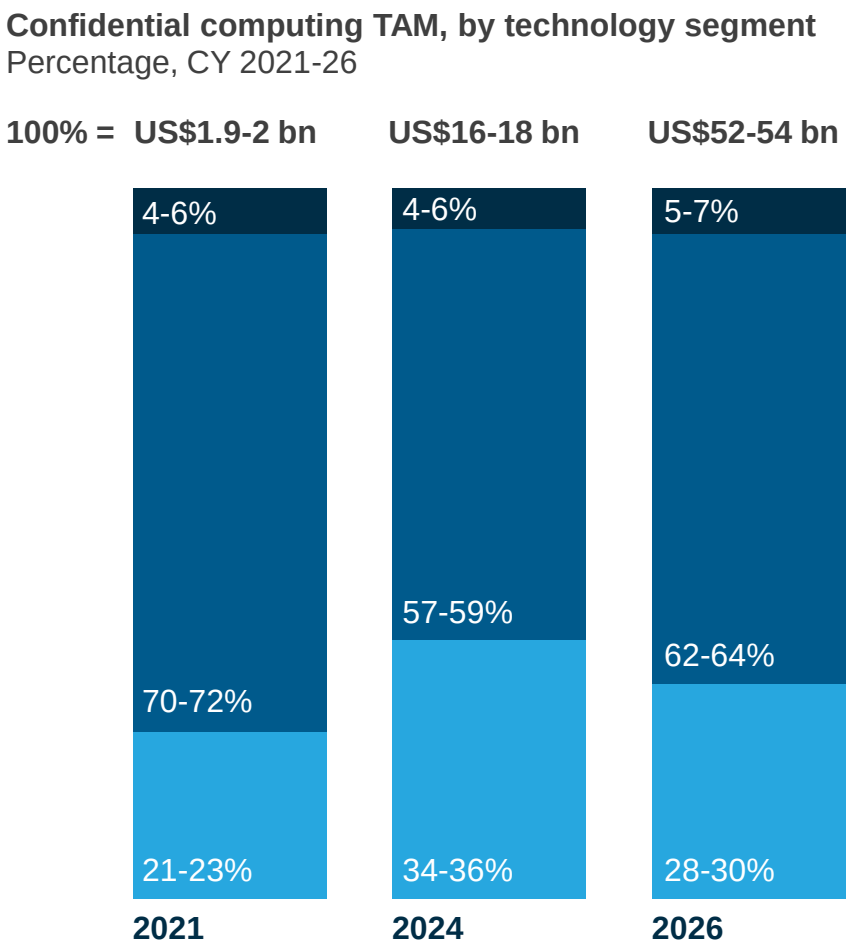
- The Total Addressable Market (TAM) for CC is likely to grow at least 26x over the next five years in the best-case scenario due to growing enterprise awareness of confidential computing
- The CC hardware and software markets are poised for exponential growth backed by expanding regulations, demand for comprehensive security postures, and appetite for new revenue generators
- Multi-party computing and security-specific use cases across industries will be the biggest growth drivers for the technology
- Technology-first enterprises within regulated industries such as banking, financial services, insurance, healthcare, and life sciences expected to drive growth acceleration across ~60% of the market
- Large technology markets in North America and APAC (ex-China) constitute the lion's share of the market followed by highly regulated markets in Europe

Confidential computing TAM
US$ billion, CY 2021-26



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



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

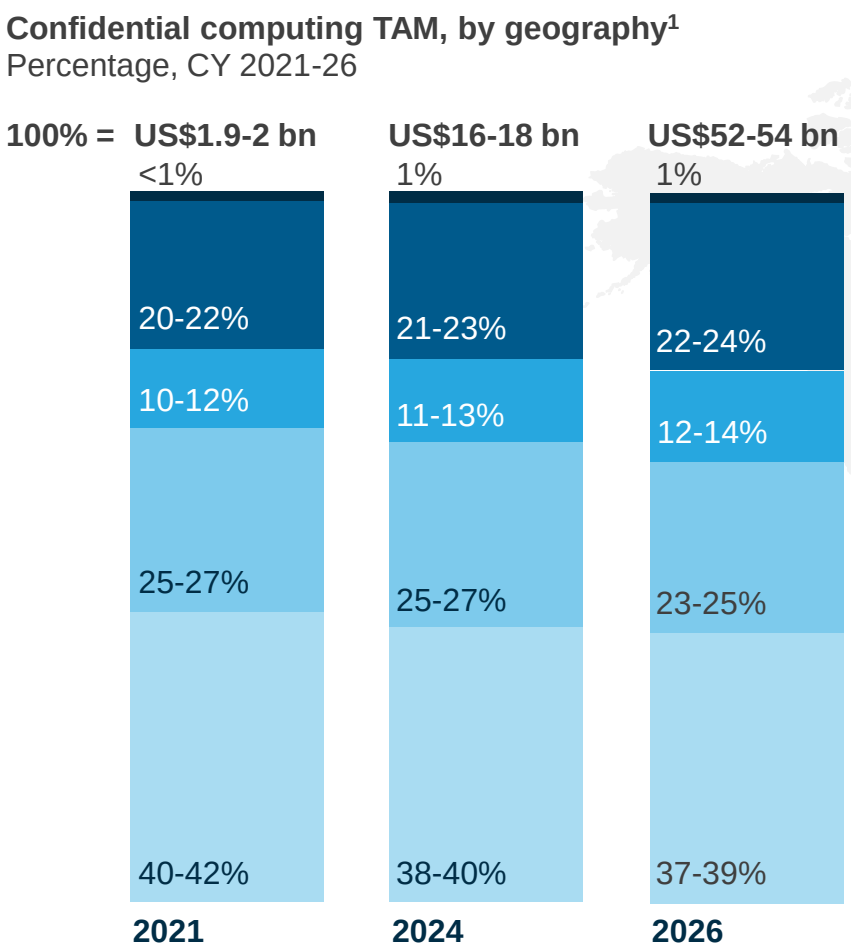
HARDWARE SUB-SEGMENTS — CAGR = 100-105%

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

Enterprises in North America and APAC (ex-China) are expected to drive the adoption of confidential computing

Confidential computing TAM, by geography[1]
Percentage, CY 2021-26



North America, China, and APAC (ex-China) are leading markets in confidential computing

- North America, China, and APAC (ex-China) account for the major share of the confidential computing market; North America's lopsided market share in 2021 is due to the strong local presence of major cloud hyperscalers in the US
- Strong security demand in these two geographies to tackle cyber threats can further push adoption of confidential computing within the enterprise ecosystem. This trend is further accelerated by government support to develop and adopt innovative cybersecurity paradigms

Country-specific data privacy regulations will play a major role

- Growing end-user awareness about data privacy is expected to play a pivotal role in deciding new government regulations, which can further drive rapid adoption of confidential computing
- Multiple countries are already contemplating newer and stricter privacy laws that define how sensitive personal data needs to be handled

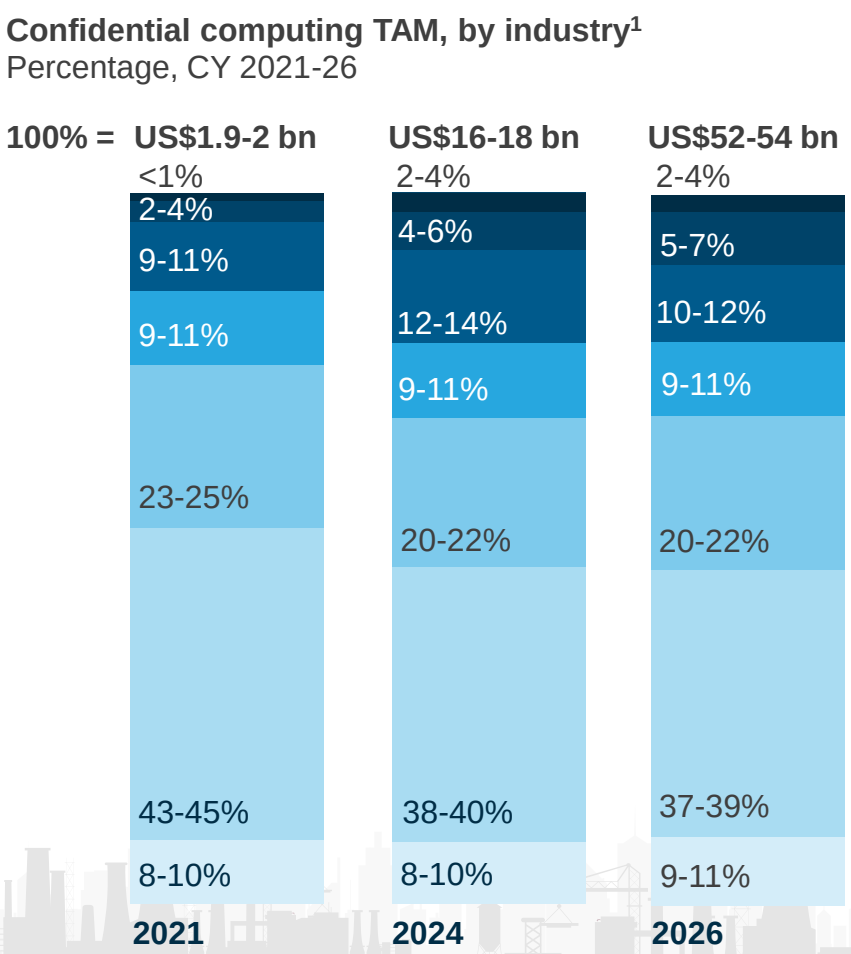
European market

- European markets such as Germany, the UK, France, Switzerland, and the Nordics are expected to drive adoption in the region
- Factors that push for regulatory compliance including GDPR, rising privacy concerns, and AI/ML adoption use cases will drive growth in the region

1 Refer to the appendix for geography cluster definitions

BFSI and Hi-tech contributes to almost 70% of the total addressable market for confidential computing; manufacturing and retail will gain traction over next few years

Confidential computing TAM, by industry[1]
Percentage, CY 2021-26



Highly regulated industries to cautiously lead adoption of confidential computing

- Driven by the need to protect critical data against attacks, industries like BFSI and HLS are expected to adopt confidential computing more aggressively than other enterprises
- The high occurrence of legacy applications and low awareness among enterprises is expected to slow demand in banking and insurance
- However, technology-first firms, particularly in the FinTech, HealthTech, and InsurTech spaces, are expected to lead the pack

Retail and manufacturing enterprises are expected to unlock shared revenue though confidential computing

Confidential computing in retail and manufacturing is expected to enhance supply chain visibility and improve collaboration among stakeholders across the value chain

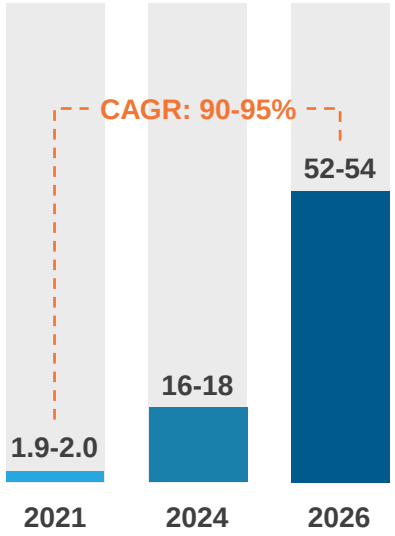
Hi-tech industry verticals are expected to follow the first phase of adoption

Given the hi-tech industry's dependence on data and analytics-based processes, IOT / edge computing, and likelihood of cyber attacks, confidential computing is expected to gain traction over the next few years

1 Refer to the appendix for industry cluster definitions

The total addressable market for confidential computing is expected to grow at least 6x in the worst case and 26x in the best case over the next five years

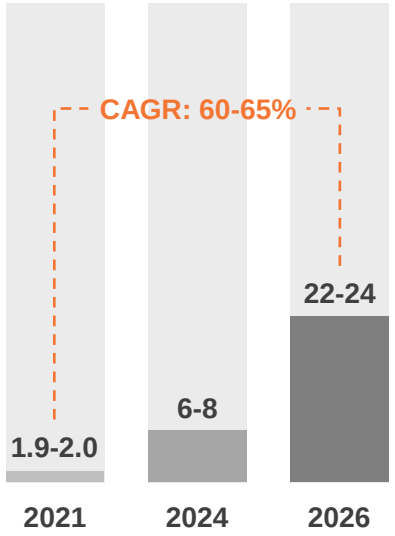
Confidential computing TAM, best case
US$ billion



Best case scenario

- The confidential computing market grows exponentially on the heels of an aggressive regulatory push and enterprise clarity on where to invest
- Vendors aggressively educate the market on use cases that drive business value and that can utilize software abstraction
- Confidential computing technology achieves high maturity and becomes equally affordable and scalable as cloud computing

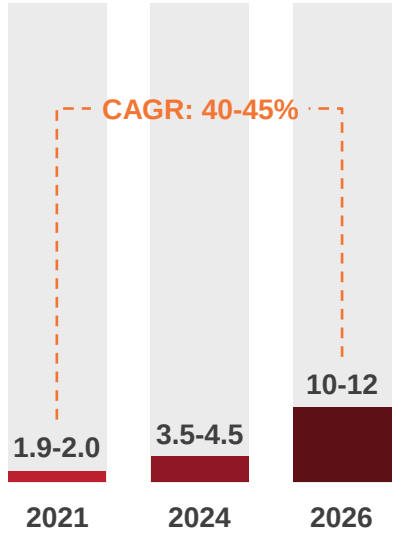
Confidential computing TAM, median case
US$ billion



Median case scenario

- A mild regulatory push to secure data in use across industries such as BFSI, HLS, and hi-tech creates growth opportunities
- Limited awareness of technology and low willingness to invest due to limited proof points and vendors' confused market messaging
- Confidential computing technology achieves relatively less maturity and is not affordable on par with cloud computing

Confidential computing TAM, worst case
US$ billion

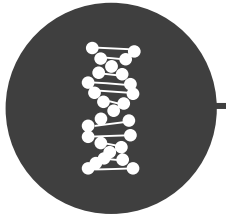


Worst case scenario

- Market confusion reigns due to poorly defined value propositions and lack of all-encompassing use cases
- Limited regulatory push to secure data in use
- Resistance to move highly secure processes that would benefit from confidential computing to the cloud combined with hurdles in talent for on-premises implementations
- High hesitance over vendor lock-in, limited standardization, and un-auditability of key vendor code bases

Industry scenario analysis | change agents for best- and worst-case market potential
(page 1 of 3)

Banking, financial services & insurance



Healthcare & life sciences

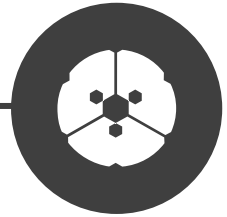
Banking, financial services & insurance confidential computing market (US$ billion)				Healthcare & life sciences confidential computing market (US$ billion)		
Best case scenario	Median case scenario	Worst case scenario		Best case scenario	Median case scenario	Worst case scenario
$0.8	$0.8	$0.8	2021	$0.5	$0.5	$0.5
$6.6	$3.0	$1.6	2024	$3.7	$1.7	$0.9
$20.4	$19.2	$4.6	2026	$11.7	$5.2	$2.6

Change agents for best case	Change agents for worst case
• Stringent data protection and residency laws • Drive to modernize core infrastructure and migration to cloud • Increased importance of data and analytics in fundamental processes • Adoption of key use cases such as blockchain and MPC	• Hesitance in moving secure processes such as key management to the cloud • High reliance on legacy applications • Higher expected cost of migrating from legacy applications and infrastructure

Change agents for best case	Change agents for worst case
• Opportunity for cross-company collaboration among providers and pharmaceuticals • Growing privacy demand for Electronic Medical Records (EMR) and real-world data collected in clinical trials • COVID-19 provides a much-needed budget push to explore new technologies	• Dependence of major pharmaceuticals and providers on legacy applications such as clinical development and EMR systems • Affinity to stay on-premises because of security risks surrounding data sensitivity • Prevalence of point solutions and high data replication/movement costs

Industry scenario analysis | change agents for best- and worst-case market potential
(page 2 of 3)

Hi-tech



Manufacturing

Hi-tech confidential computing market (US$ billion)				Manufacturing confidential computing market (US$ billion)		
Best case scenario	Median case scenario	Worst case scenario		Best case scenario	Median case scenario	Worst case scenario
$0.2	$0.2	$0.2	2021	$0.1	$0.1	$0.1
$1.5	$0.7	$0.3	2024	$0.8	$0.3	$0.2
$5.4	$2.3	$1.1	2026	$3.0	$1.1	$0.5

Change agents for best case

- High spend potential on confidential computing-enabled use cases, especially in areas of IOT / edge computing, personal computing devices, and MPC
- Strong push from telecom and network operators to build automated trust assessment of all network elements, including nodes, devices, applications and virtual resources in the cloud

Change agents for worst case

- Skepticism in moving large volumes of critical processes to confidential computing
- Slower adoption of 5G and cloud-based software-defined offerings of telecom and network operators

Change agents for best case

- Rampant adoption of security services to plug security gaps in the existing IT infrastructure estate
- Growing IT and OT convergence
- Robust digital footprint, underpinned by Industry 4.0
- Need to secure critical and expensive infrastructure against increasing cyber threats

Change agents for worst case

- Limited awareness of confidential computing and applicability of use cases
- Persistent supply chain challenges keep the leadership busy
- Lack of clarity of ROI and demonstrated proof points within the industry

Industry scenario analysis | change agents for best- and worst-case market potential
(page 3 of 3)

Public sector

Retail and CPG

Public sector confidential computing market (US$ billion)				Retail and CPG confidential computing market (US$ billion)		
Best case scenario	Median case scenario	Worst case scenario		Best case scenario	Median case scenario	Worst case scenario
$0.2	$0.2	$0.2	2021	$0.2	$0.2	$0.2
$1.8	$0.8	$0.4	2024	$2.2	$0.9	$0.5
$5.3	$2.2	$1.0	2026	$6.0	$2.6	$1.2

Change agents for best case	Change agents for worst case
• Transformation of citizen services involving critical personal data such as identification numbers and biometrics • Regulation on usage of citizen data • Rise in advanced cyber attacks on public infrastructures • Upgrades of critical defense operations to improve cyber resilience	• Prohibitive government spending owing to lingering pandemic effects and slow economic recovery • Hesitance to adopt new technology using public money with limited proof points • Sensitivity to evolving cost premium over regular technology

Change agents for best case	Change agents for worst case
• Increased regulation on customer data aggregation and analysis • Swelling appetite for inter-enterprise collaboration for optimization and new revenue generation • New commerce and sales paradigms and corresponding influx of data • Increased need for supply chain resilience	• Slower economic recovery from the pandemic • Pressure on traditional retailers from ecommerce as value and price sensitivity rise • Hesitance in adopting collaborative analytics principles such as MPC

04

Enterprise demand trends

- Factors driving the confidential computing market spend
- Use cases gaining market traction

Enterprise awareness | heavy exposure to sensitive data and increasing regulatory scrutiny necessitate high awareness among regulated industries

Not exhaustive

Enterprise awareness trend for confidential computing over the next five years

Industry	Awareness factor[1] (% of enterprises aware of CC)			Key use cases driving enterprise spend
	2021	2024	2026	
BFSI	13-15%	23-25%	29-31%	Collaborative analytics for anti-money laundering and fraud detection, secure DeFi access, privacy in blockchain transactions, privacy in ML and federated learning, data exchanges/ marketplaces
HLS	13-15%	23-25%	27-29%	Research and analytics on patient data, drug discovery, and treatment modeling, and security for IoT devices
Public sector	9-11%	14-16%	17-19%	Citizen data analytics, cross-agency collaboration, predictive maintenance of military equipment, security for publicly exposed assets

- Regulated industries are more open to exploration into and experimentation with security-enhancing technologies such as confidential computing because they have been facing an increasing push to improve data security and privacy from regulators. High exposure to private data coupled with regulations such as CCPA, Schrems II, GDPR, and HIPPA ensure that interest in confidential computer will be high among BFSI and HLS enterprises
- In addition, the technology-first FinTech, Insurtech, and HealthTech firms are likely to push awareness of confidential computing in BFSI and HLS over the next five years

1 Awareness factor is a quantitative estimate of the percentage of enterprises that are aware of confidential computing and related business implications. These are the enterprises that are willing to spend in confidential computing, which we call “aware” enterprises in this study. Refer to the appendix for details.

Enterprise awareness | growth in awareness among less regulated industries will be driven by the need to secure personal data and the thirst for new revenue

Not exhaustive

Enterprise awareness trend for confidential computing over the next five years

Industry	Awareness factor[1] (% of enterprises aware of CC)			Key use cases driving enterprise spend
	2021	2024	2026	
Hi-tech	11-13%	17-19%	21-23%	Key management, client data protection, federated learning, multi-party analytics, IoT/Edge device and data security, IP protection
Retail and CPG	8-10%	17-19%	22-25%	DLT-based tracking and provenance, buyer-supplier data analytics, new business models from multi-party computing, edge computing
Manufacturing	4-6%	11-13%	14-16%	DLT-based tracking and provenance, buyer-supplier data analytics, real-time analytics, edge computing, computation of encrypted data for autonomous vehicles, IP protection

- Among less regulated industries, awareness is likely to accelerate in the hi-tech and retail/CPG verticals. The hi-tech and CPG sectors, particularly telecom and consumer electronics enterprises, are expected to explore confidential computing across key IoT/edge and personal device use cases to drive hyper-personalization
- Meanwhile, manufacturing enterprises are expected to adopt confidential computing to supplement collaborative use cases such as Multi-Party Computing (MPC) and real-time supply chain tracking/provenance

1 Awareness factor is a quantitative estimate of the percentage of enterprises that are aware of confidential computing and related business implications. These are the enterprises that are willing to spend in confidential computing, which we call “aware” enterprises in this study. Refer to the appendix for details.

Applicability of confidential computing to enterprise IT portfolios will accelerate as the ecosystem matures and awareness of benefits increases over the next five years

Privacy Preserving Potential (PPP)[1] across industries over the next five years

Industry	PPP in 2021	PPP in 3 years	PPP in 5 years
BFSI	1.5-2.5%	5-6%	10-12%
HLS	1.5-2.5%	4.5-5.5%	10-12%
Public sector	1-2%	3-4%	5-7%
Hi-tech	1-2%	3-4%	7-9%
Retail and CPG	0.5-1%	2.5-3.5%	4-6%
Manufacturing	0.5-1%	2-3%	4-6%

- PPP is a quantitative factor that determines the spending potential of enterprises that are aware of confidential computing. It includes various qualitative factors such as willingness of executives to spend on confidential computing and business imperatives
- Regulated industries like BFSI and HLS are likely to have higher PPP percentage growth in the long run given the sensitivity of the data they handle
- Despite high applicability on citizen and defense data, public sector PPP is expected to remain low due to significant use of legacy applications and subsequent cost to change
- Among less regulated industries, telecom is expected to have high degree of applicability on its distributed infrastructure. The Retail/CPG sector, led by e-commerce giants, will have a strong appetite to adopt confidential computing to secure sensitive personal data

1 The percentage of applications from the overall application portfolio where “aware” enterprises are willing to invest is referred to as PPP in this document. PPP is estimated at each industry level. Refer to the appendix for details

Use case assessment | assessment methodology

As a part of this market report we have analyzed more than 50 confidential computing use cases and have classified them into five broad categories[1]: **privacy and security, blockchain, multi-party computing, IoT and edge, and personal computing devices.** We have further assessed these use cases based on market traction and future potential; the table below explains the assessment criteria used.

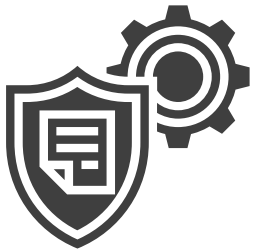
Key terminology	Everest Group definition	Assessment rating – high	Assessment rating – low
Market traction	Qualitative estimate gradient that highlights the current adoption of a certain use case among enterprises in the market	• Relatively good spread of clients exploring the use case • High awareness of usage among enterprises and demonstrated business value • Strong interest for joint developments and partnerships	• Use cases being explored by a narrow subset of clients • Limited awareness among enterprises • Limited exploration of use cases among ISVs • Business value demonstrated is sparse
Future potential	Qualitative estimate gradient that conveys the extent of possible future adoption of a certain use case, in a best-case scenario in 2026	• Lower barrier to entry • Large potential base market for the use case • Radical use cases with ability to establish new market segments	• High degree of difficulty and risk in change management • Niche applicability of use case

1 Refer to the appendix for detailed use case definition

Enterprises are exploring a wide range of use cases enabled by confidential computing working alongside key market makers of the industry

Not exhaustive

Key use case categories enterprises are exploring

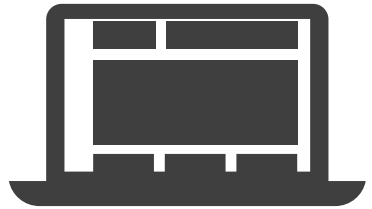


Privacy and security

Blockchain

Multi-party computing

IoT and edge



Personal computing devices

Privacy and security | confidential computing has broad applicability across privacy and security

Market contribution (2021)
30-35%

Market growth (5-year CAGR)
100-110%

Low → High

Future potential of use case	■■■■■

Market traction across industries

BFSI	■■■■■
HLS	■■■■□
Hi-tech	■■■■■
Manufacturing	■□□□□
Public sector	■■■□□
Retail and CPG	■■□□□

Use case scenarios[1]	Description
Key management system	• Traditionally, enterprises have preferred to keep KMS control within their on-premises datacenters. However, with the growing popularity of zero trust architecture and awareness of confidential computing, this preference is slowly diminishing • Confidential computing provides a robust, cloud-friendly, scalable, and distributed KMS architecture; there are already service offerings for this use-case
Application security on public cloud	• Enterprises have always been skeptical about security related to deploying applications on public cloud, primarily because of fears of hackers gaining unauthorized access to sensitive data and/or malicious insider attacks, and data privacy concerns • Confidential computing enables applications to run in an isolated, hardware protected, and attestable environment, which not only enhances the overall application security but also curtails data privacy risks

Notable adopters

adidas PayPal Signal ZAFIN

1 Refer to the appendix for detailed use case definition

Blockchain | confidential computing can improve network data privacy and improve long-term sustainability of blockchains

Market contribution (2021)	23-27%
Market growth (5-year CAGR)	65-70%

Low → High

Future potential of use case	

Market traction across industries

BFSI	
HLS	
Hi-tech	
Manufacturing	
Public sector	
Retail and CPG	

Use case scenarios[1]	Description
Meaningful Proof of Work	• Current PoW algorithms use significant resources for computations required to write to a network and maintain wallets • Confidential computing focuses these resources on meaningful work such as scientific research simulation or modelling instead of current mathematical computations to improve resource efficiency and network sustainability
Blockchain data privacy	• Blockchain services and applications can offer private data and secured transactions for authorized network participants when the infrastructure is implemented using confidential computing • Currently, most popular explorations of blockchain using confidential computing include secure voting systems, private auctions, anti-money laundering, fraud detection, KYC, and digital finance

Notable adopters

intellect EU · MobileCoin · Santander · JCB

1 Refer to the appendix for detailed use case definition

Multi-party computing | confidential computing has opened new doors to collaborative analysis and modeling

Market contribution (2021)
18-23%

Market growth (5-year CAGR)
145-150%

Low → High

Future potential of use case	■■■■□

Market traction across industries

BFSI	■■■■■
HLS	■■■■□
Hi-tech	■■■■□
Manufacturing	■■■□□
Public sector	■□□□□
Retail and CPG	■■■■□

Use case scenarios[1]	Description
Private data sharing	• Private or regulated data can be shared safely across enterprises with the guarantee of encryption across data storage, transmission, and processing. Such data sharing opens new avenues of collaboration and revenue generation for enterprises • Examples include clinical trials, sharing of Real World Data (RWD) by healthcare providers, and Swiss banks sharing data outside of Switzerland
Multi-party analytics	• Enterprises can unlock new insights by collaboratively pooling and analyzing data across market participants. Confidential computing considerably reduces the risk of exposing sensitive data during analysis and enhances compliance to regulations • Examples include fraud detection in BFSI, collaborative scientific research, conducting market studies, and customer data analysis across firms
Privacy-preserving AI/ML modeling	• Confidential computing helps keep the input data and output model secure throughout the training process • Currently, the majority of modeling and simulations are conducted on data aggregated at a centralized location. MPC also enhances the value proposition for decentralized modeling techniques such as federated learning, wherein each node executes processes on a TEE

Notable adopters

CREDIT SUISSE · LYNXCARE · RBC · swisscom · UCSF University of California San Francisco

1 Refer to the appendix for detailed use case definition

IoT and edge | confidential computing helps maintain the integrity and control of IOT and edge devices

Market contribution (2021)
5-10%

Market growth (5-year CAGR)
55-60%

Low → High

Future potential of use case	■■□□□

Market traction across industries

BFSI	■□□□□
HLS	■□□□□
Hi-tech	■■□□□
Manufacturing	■■■□□
Public sector	■□□□□
Retail and CPG	■■□□□

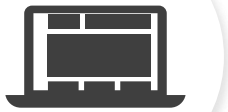
Use case scenarios[1]	Description
Trusted command and control	• Ensures only authorized commands and code are executed by edge and IOT devices. Use of confidential computing at the IOT and edge devices and back end helps control critical infrastructure by preventing tampering with code of data being communicated across interfaces • Examples include execution of critical functions in autonomous cars
Secure data and IP	• Confidential computing in a distributed edge network can also help realize new efficiencies without affecting data or IP privacy by building a secure foundation to scale analytics at the edge without compromising data security • Examples include handling automotive data at workshops without exposing sensitive IP of components or transferring proprietary data to partner clouds

Notable adopters

BOSCH ERICSSON

1 Refer to the appendix for detailed use case definition

Personal computing devices | the end-user can enjoy a high degree of personalization without apprehensions around transmission and use of personal data



Market contribution (2021)
3-7%

Market growth (5-year CAGR)
25-30%

Low → High

Future potential of use case	

Market traction across industries

BFSI	
HLS	
Hi-tech	
Manufacturing	
Public sector	
Retail and CPG	

Use case scenarios[1]	Description
Personalized recommendations	• Confidential computing lays a foundation for the processing of personal data on private devices without ever sending the data to a central server. This results in a variety of new features such as personalized replies and recommendations using ML models trained on local data • Android recently rolled out a new feature called Android Private Compute Core to serve the personalized recommendation use-case; on the downside, it is a software-level partitioning, which lowers the level of data protection and cannot be categorized as confidential computing • However, in the future we anticipate new chipsets being announced for confidential computing that can bring hardware-level partitioning solutions to personal computing devices

Notable adopters

1 Refer to the appendix for detailed use case definition

05

Implications

- Implications for enterprises
- Implications for technology and service providers

Implications for enterprises

Start exploring	Invest in talent	Scale up
In the next 6-12 months enterprises across industry verticals should build a business case for confidential computing by developing proofs of concept specific to their enterprise contexts. The focus should be on identifying applications where confidential computing is needed and urgent.	As the market matures, talent supply growth will not keep up with talent demand. Enterprises should start to invest in upskilling the existing talent to bridge this talent gap.	Confidential computing will become the standard approach to ensure end-to-end security of data in business-critical applications. After identifying these applications at the proof of concept stage, enterprises should partner with technology and service providers to scale up adoption in the next three to five years.

Implications for technology and service providers

Software providers	Hardware providers	IT service providers
Software providers will play a pivotal role in ensuring technology maturity and simplifying consumption of confidential computing. While hyperscalers need to make the technology more affordable, other software enablers should introduce the industry-specific context.	The confidential computing market's expected growth of about 100% CAGR over the five years will be hugely dependent on the availability of required hardware. Enterprises are likely to adopt confidential computing across public and private cloud offerings, which presents a massive opportunity for hardware vendors.	Service providers will play a major role in improving enterprise awareness of confidential computing. They need to guide enterprises by creating business use cases and investing proactively in developing proofs of concept.

06

Appendix

- Key definitions used in the market opportunity assessment
- Use case definition

Key definitions used in the market opportunity assessment (page 1 of 2)

Key terminology	Everest Group definition
Awareness factor of enterprises within industries	Awareness factor is a quantitative estimate of the percentage of enterprises that are aware of confidential computing and its related business implications. These are the enterprises that are willing to spend in confidential computing; we refer to them as “aware” enterprises in this study. For example, a 10% awareness factor for the BFSI industry means that 10% of BFSI enterprises are aware of the business case for confidential computing and are willing to spend money on it.
Privacy Preserving Potential (PPP) of IT portfolio	PPP is the percentage of applications from the overall application portfolio in which aware enterprises are willing to invest. We have estimated PPP at each industry level. For example, a 3% PPP in BFSI means that in any aware BFSI enterprise, 30 in 1,0000 applications are considered an absolute must to transition to confidential computing.

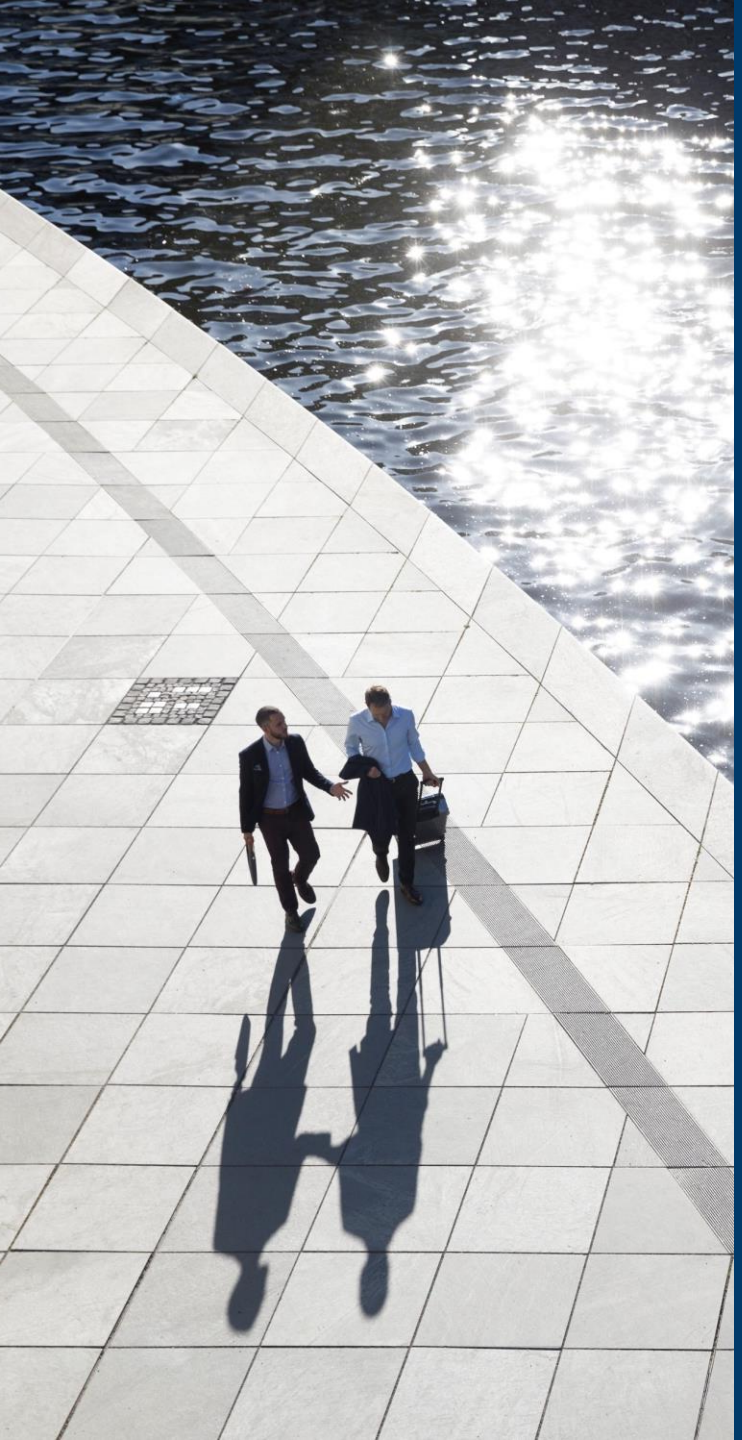
Key geography	Everest Group definition
APAC (excludes China)	Asia-Pacific; includes, India, the Middle-East, Australia, New Zealand, and other Asia-Pacific countries, excluding China
China	Includes the People’s Republic of China
North America	Includes the US, Canada, and Mexico
Europe	Includes all regions in Europe across the UK and Ireland, Western, Central, and Eastern Europe and the Nordics
RoW	Rest of the world; primarily includes Central America, South America, and Africa

Key definitions used in the market opportunity assessment (page 2 of 2)

Key industries	Everest Group definition
Hi-tech	Includes Independent Software Vendors (ISVs), electronics, and telecommunications; excludes technology-focused firms such as those in FinTech, InsurTech, HealthTech, and e-commerce among others
BFSI	Includes the banking, financial services, and insurance industries; also includes FinTechs and InsurTechs
HLS	Includes the healthcare and life sciences industries; also includes HealthTech firms and life sciences tech enterprises
Public sector	Includes government organizations, particularly citizen services and defense
Retail & CPG	Retail and Consumer Packaged Goods (CPG) includes companies selling consumable and durable goods, such as food, cookware, appliances, Fast Moving Consumer Goods (FMCG), and fashion as well as retail and distribution networks that sell them; also includes all the e-commerce enterprises
Manufacturing	Includes companies in discrete manufacturing such as automobiles and industrial equipment and process manufacturing segments such as steel and cement
Others	Includes industries outside the scope of the above classifications such as energy, utilities, travel, transportation, hospitality, and education, among others

Use case definition | Major uses that are gaining traction in the market

Use case	Sub-use case	Everest Group definition
Privacy and security	Key management system	Confidential computing used to secure systems that deal with the generation, exchange, storage, and use of cryptographic keys used across the enterprise IT landscape
	Application security on public cloud	Confidential computing used in typical cloud scenarios such as containers or microservices applications to prevent the compromise of data from malicious actors and proactively improve an application's security and privacy posture
Blockchain	Meaningful Proof of Work (PoW)	PoW is a cryptographic concept in blockchain that helps one party prove to others in a blockchain network that a certain amount of a specific computational effort has been expended; this effort can then be verified through minimal effort on the blockchain. Meaningful proof of work is a technique of PoW where the computational effort required is utilized for productive purposes
	Blockchain data privacy	Confidential computing used to secure data being written or processed on the blockchain network to add an additional element of privacy to the system
Multi-party computing	Private data sharing	Utilization of confidential computing by an entity such as a hospital or bank, to share sensitive data, such as patient or financial data with third parties such as pharmaceutical companies, insurers, or credit rating agencies
	Multi-party analytics	Use of confidential computing by multiple entities aggregating their proprietary data and collaboratively analyzing it to gain new insights
	Privacy-preserving AI/ML modeling	Use of confidential computing to secure data during the modeling and training of AI; further confidential computing is used to secure modeling in decentralized training mechanisms such as federated learning
IoT and Edge	Trusted command and control	Confidential computing used to protect critical infrastructure connected to the internet to prevent malicious entities from accessing, controlling, or manipulating key devices, sensors, or systems
	Secure data and IP	Use of confidential computing to secure intellectual property and data generated or utilized in edge and IOT devices from malicious elements
Personal computing devices	Personalized recommendations	Confidential computing used on personal computing devices to analyze data and build models on the device to reduce the need for off-device or cloud processing



Everest Group®
With you on the journey

Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our clients include leading global companies, service providers, and investors. Clients use our services to guide their journeys to achieve heightened operational and financial performance, accelerated value delivery, and high-impact business outcomes. Details and in-depth content are available at **www.everestgrp.com**.

Stay connected

Website
everestgrp.com

Social Media
@EverestGroup
@Everest Group
@Everest Group
@Everest Group

Blog
everestgrp.com/blog

Dallas (Headquarters)
info@everestgrp.com
+1-214-451-3000

Bangalore
india@everestgrp.com
+91-80-61463500

Delhi
india@everestgrp.com
+91-124-496-1000

London
unitedkingdom@everestgrp.com
+44-207-129-1318

Toronto
canada@everestgrp.com
+1-647-557-3475

This study was funded, in part, by **Confidential Computing Consortium**