Trust. Data. AI.

Co-create new business with you, powered by Confidential Computing

Takeharu Kondo

Co-Founder & Executive Officer

Obstacles to Leveraging SaaS/AI for Business

Data Breach Risks

32% cite **data breach risks** as a **barrier to cloud adoption**

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252140.html

Security Matters in Healthcare

45% fear **security risks** in **healthcare cloud systems**

https://mnes-lookrec.com/news/40

Confidentiality First in Finance

37% face **confidentiality Issues in Finance**

https://www.boj.or.jp/research/brp/fsr/data/fsrb240130c.pdf

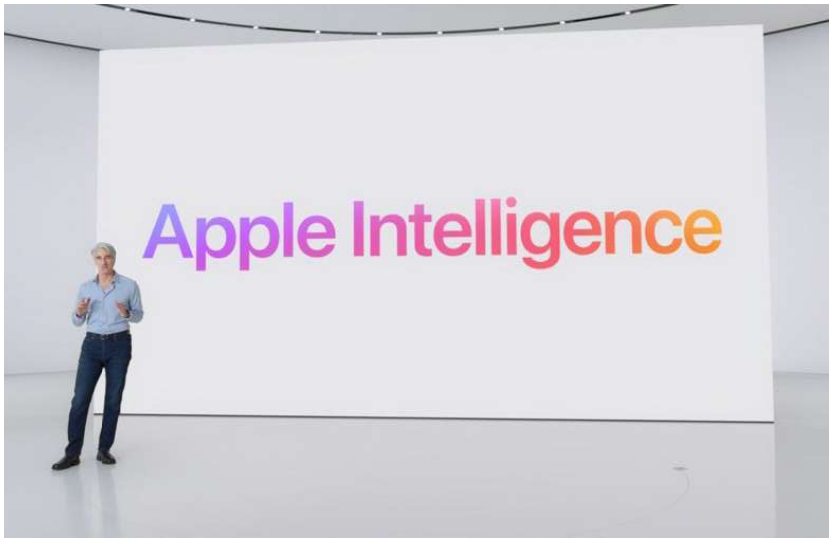
Data Security Risks Limit Growth and Market Potential.

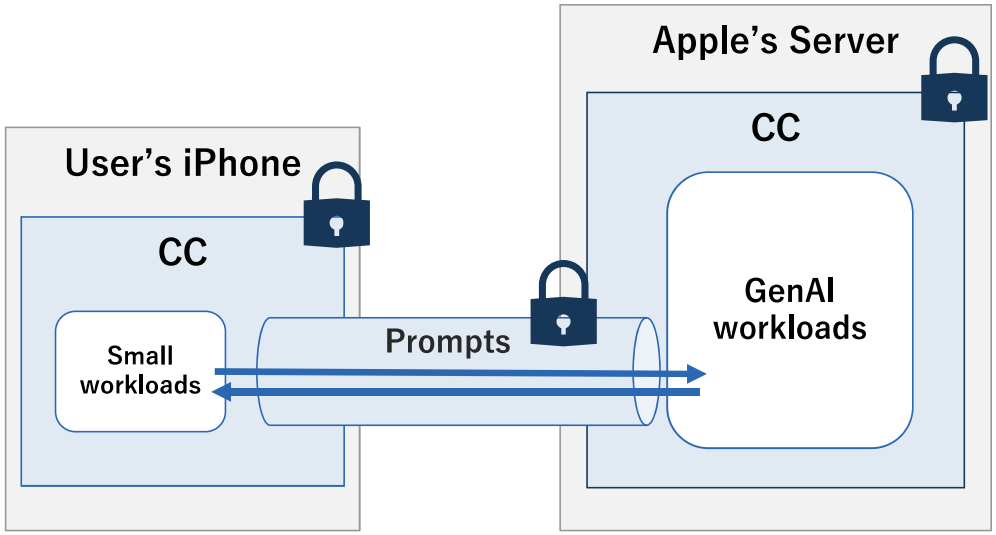
The Solution

Unlock the Full Potential of Data with Confidential Computing

Keep all data safe while you use it.

Apple uses Confidential Computing for their GenAI systems





Apple has no access to user's private prompts.

https://developers.googleblog.com/ja/enabling-more-private-gen-ai/

Our Product

Your App, Instantly Upgraded.

Retrofits your apps with data security, anytime.

Our Core Product is Based on Joint Research with Intel Labs.

Securing Nested Attestation of Confidential Serverless Computing without Intra-Enclave Isolation

Atsuki Momose
Acompany Co., Ltd.
atsuki.momose@acompany-ac.com

Kailun Qin
Intel & Shanghai Jiao Tong University
kailun.qin@intel.com

Ao Sakurai
Acompany Co., Ltd.
ao.sakurai@acompany-ac.com

Mona Vij
Intel Labs
mona.vij@intel.com

ABSTRACT

Confidential Computing-as-a-Service has gained significant attention in recent years, driven by rapid advances in Trusted Execution Environment (TEE) technology. Among various architectures, confidential serverless computing has emerged as a promising model. A common approach to designing confidential serverless computing involves decoupling the client workload from the initial enclave image and dynamically provisioning the workload at runtime. This enables both offloading the costly enclave bootstrapping and maintaining a fixed reference measurement for attestation. This decoupling necessitates *nested attestation*, where the client's workload is attested via a custom attestation module embedded in a platform-attested enclave established at boot time. The challenge in designing nested attestation, however, is to distinguish fresh

1 INTRODUCTION

Confidential Computing-as-a-Service (CCaaS) [7, 44] is a form of cloud service model where the cloud service provider (CSP) offers *secure enclaves*, typically backed by hardware-assisted Trusted Execution Environment (TEE) technology, allowing users to run workloads in an isolated execution environment that remains protected from system software, hypervisors, and even cloud administrators. Common TEE technologies include Intel SGX [11, 28] and Intel TDX [17], AMD SEV [3], and ARM CCA [24]. These technologies typically provide tamper-proof attestation features, allowing remote clients to verify both the hardware specifications and the exact software running within the enclave. This ensures remote clients can securely execute their workloads even against a potentially malicious CSP.

https://eprint.iacr.org/2025/727.pdf

Trusted by Leading Enterprises

Data Collaboration

Digital Marketing

Hakuhodo DY holdings

Authentication

TOPPAN

Medical AI

名古屋大学医学部附属病院
NAGOYA UNIVERSITY HOSPITAL

東北大学病院
TUH

北海道大学病院
HOKKAIDO UNIVERSITY HOSPITAL

Manufacturing

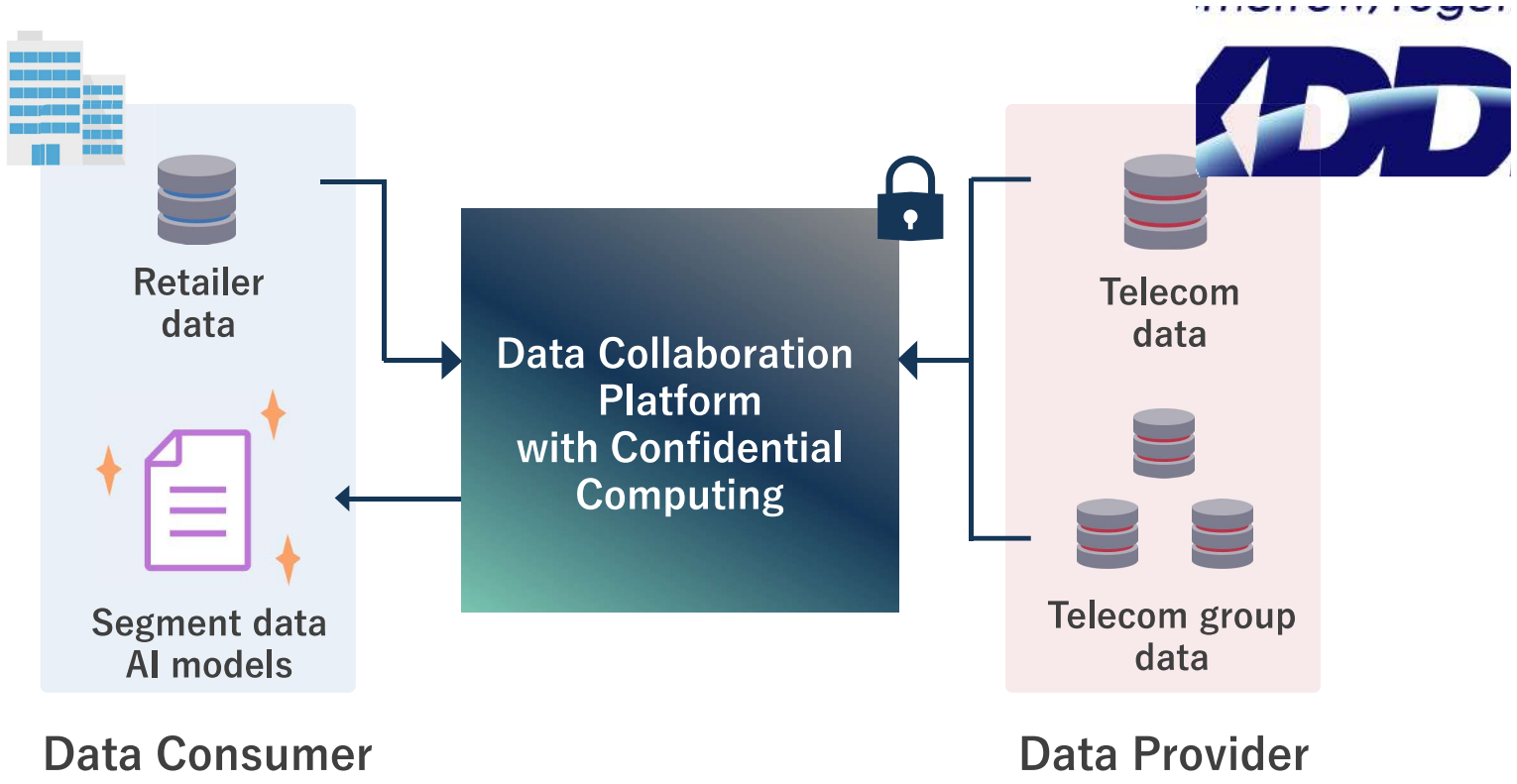
Alxtal

National Security

Major System Integrator

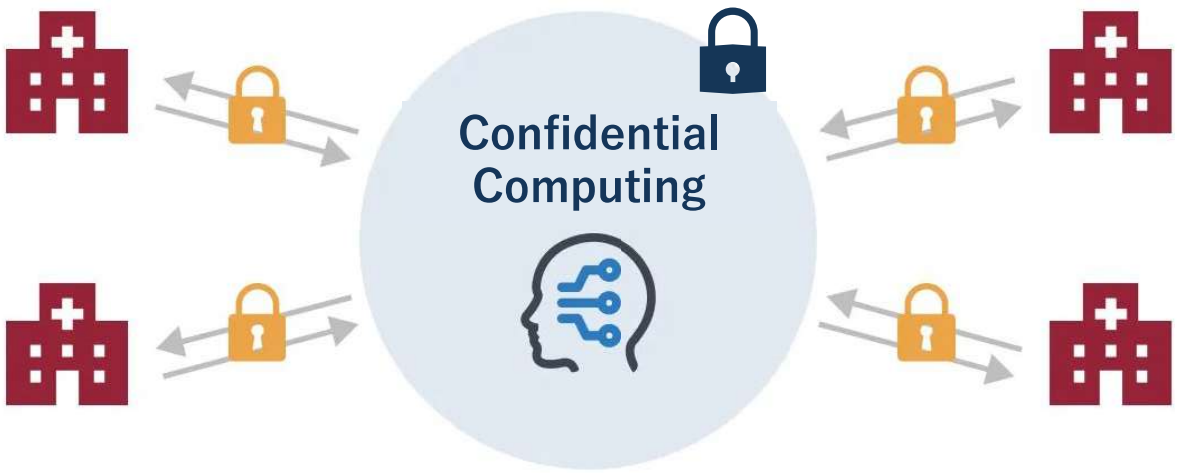
User Case: Data Collaboration

The Telco Launched a New Data Business that Safeguards Data in Use.



User Case: Medical AI

Collaborative AI Model Training for Medical Research Use



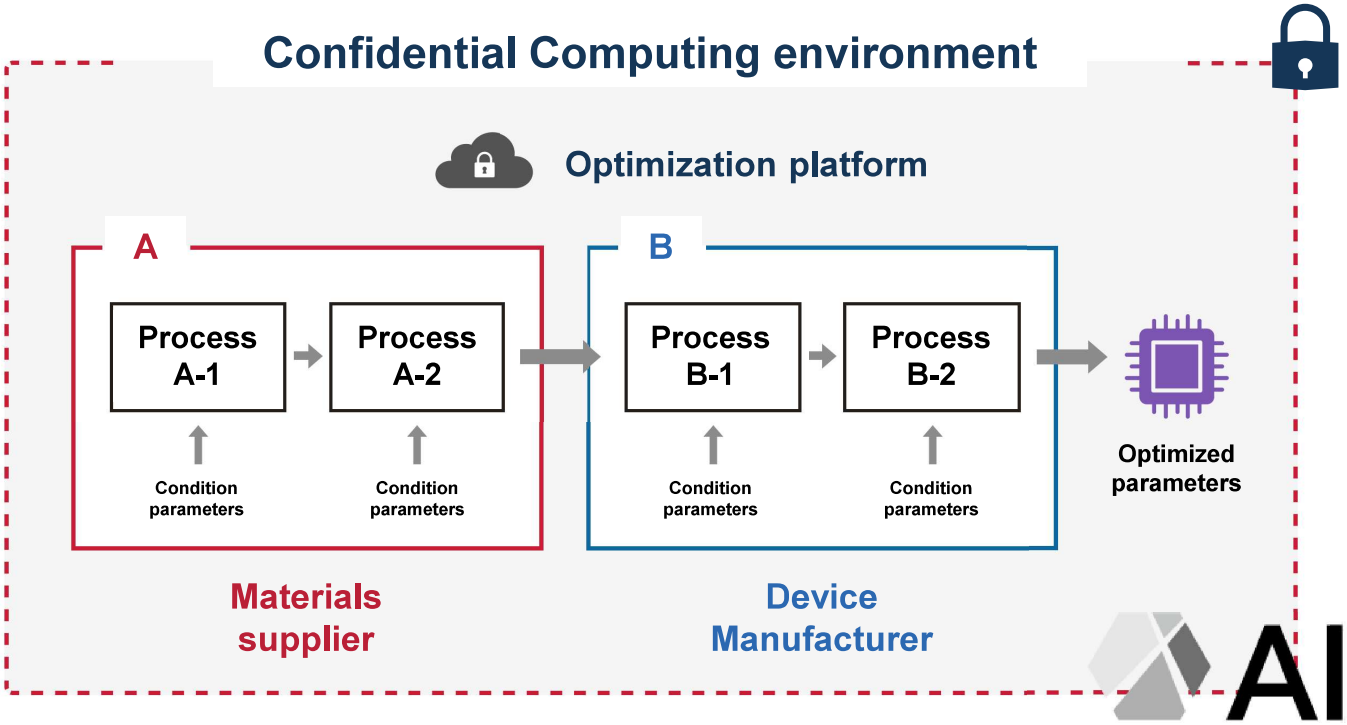
名古屋大学医学部附属病院
NAGOYA UNIVERSITY HOSPITAL

TUH 東北大学病院

北海道大学病院
HOKKAIDO UNIVERSITY HOSPITAL

User Case: Manufacturing

Optimizing Manufacturing without Exposing Data and AI Models.



Japan's Top R&D and BizDev Team in Confidential Computing

Managements

Engineers from Nagoya Univ./Nagoya Tech and ex-global consultants & mega bank members.

Ryosuke Takahashi

名古屋大学 30

R&D

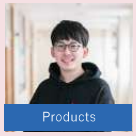
Takeharu Kondo

名古屋工業大学

BizDev

Reiji Sato

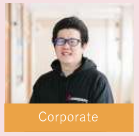
accenture



Products

Raiki Tanaka

名古屋大学



Corporate

Hayata Sagasaki

MUFG

BizDev

Hiroki Hashimura

accenture

Confidential Computing R&D

LINEヤフー

NEC

Takao Takenouchi

Leading experts in the CC

- NEC→Digital Garage→LINE Yahoo
- Founded "Confidential Computing Research Group" and "DSA Confidential Computing WG"
- Appointed to expert committees, including the Digital Agency

MITOU IBM

Ao Sakurai

Japan's top CC Researcher

- Mitou Super Creator for TEE research
- SecCamp National Instructor (2023–)

Leading in security

SECOM

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Atsuki Momose

Former PhD Researcher at University of Illinois, and a top young researcher in Confidential Computing in Japan

- Ex-SECOM → University of Illinois
- 5 first-author papers at ACM CCS for 4 consecutive years (Japan's top).
- Selected as "CCS 2024 Top Reviewer."
- Awarded "Illinois Distinguished Fellowship."
- Received Ethereum Foundation Research Grant for Confidential Computing.

Members

accenture Microsoft NEC LINEヤフー SAP SCSK NOMURA 個人情報保護委員会 Personal Information Protection Commission SECOM Digital Garage EXAWIZARDS

pwc MUFG FAST RETAILING IBM MACQUARIE Deutsche Bank Group citi bank ORACLE M3, Inc. TREASURE DATA

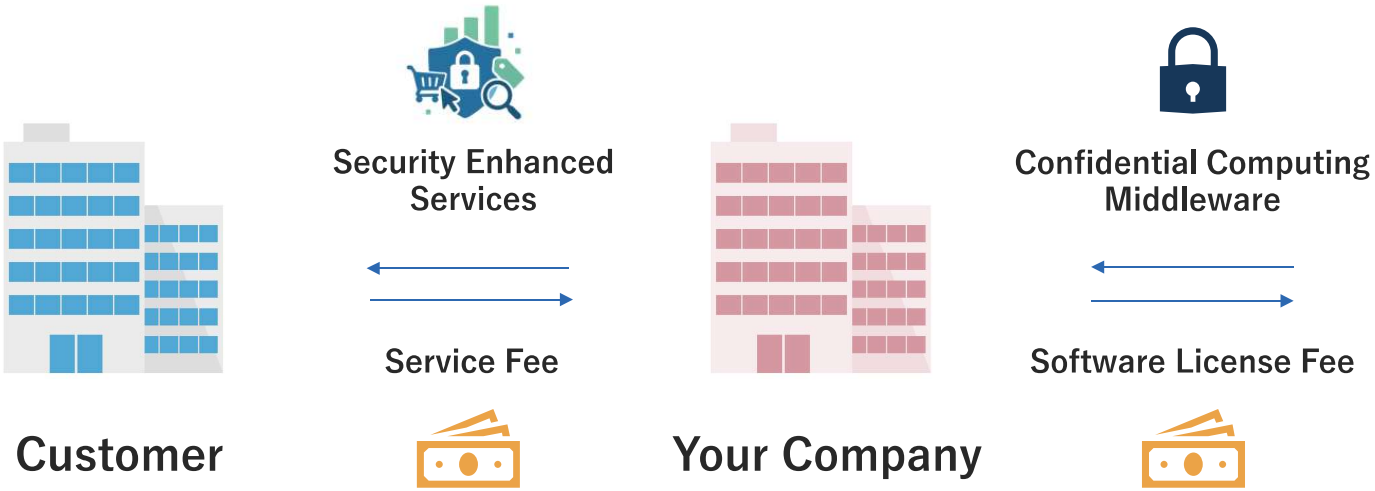
Go-to-Market Strategy

Security as Your Unfair Advantage

Target Market	Our Joint Solution	Why We Win
FinTech	Your FinTech App + Confidential Computing	Improve fraud detection by securely sharing financial data/AI without exposing them.
HealthTech	Your HealthTech App + Confidential Computing	Accelerate drug discovery for Pharma, protecting users' privacy.
National Security	Your National Security Solution + Confidential Computing	Protect National AI assets from Cyber Threats.

The Partnership Model

Co-Growth Model: Creating New Markets Together



The Special Offer 🎁

A 2-Week “Zero-Risk” PoC.

1. Prepare	2. Deploy	3. Check
• Choose one of your applications(Includes: Docker containers, Programs, AI Models)	• Our engineers will deploy them into a confidential environment.	• Your team gets full access to test, validate, and benchmark the performance and security.

Try It Free for 2 weeks!

Next Steps

Let’s Create the Next Step.

NDA

- To allow for a deeper technical and comercial discussion

Free PoC

- Jointly define the success criteria for the 2-week PoC.

Launch the Partnership

- And begin building the partnership

Thank you!

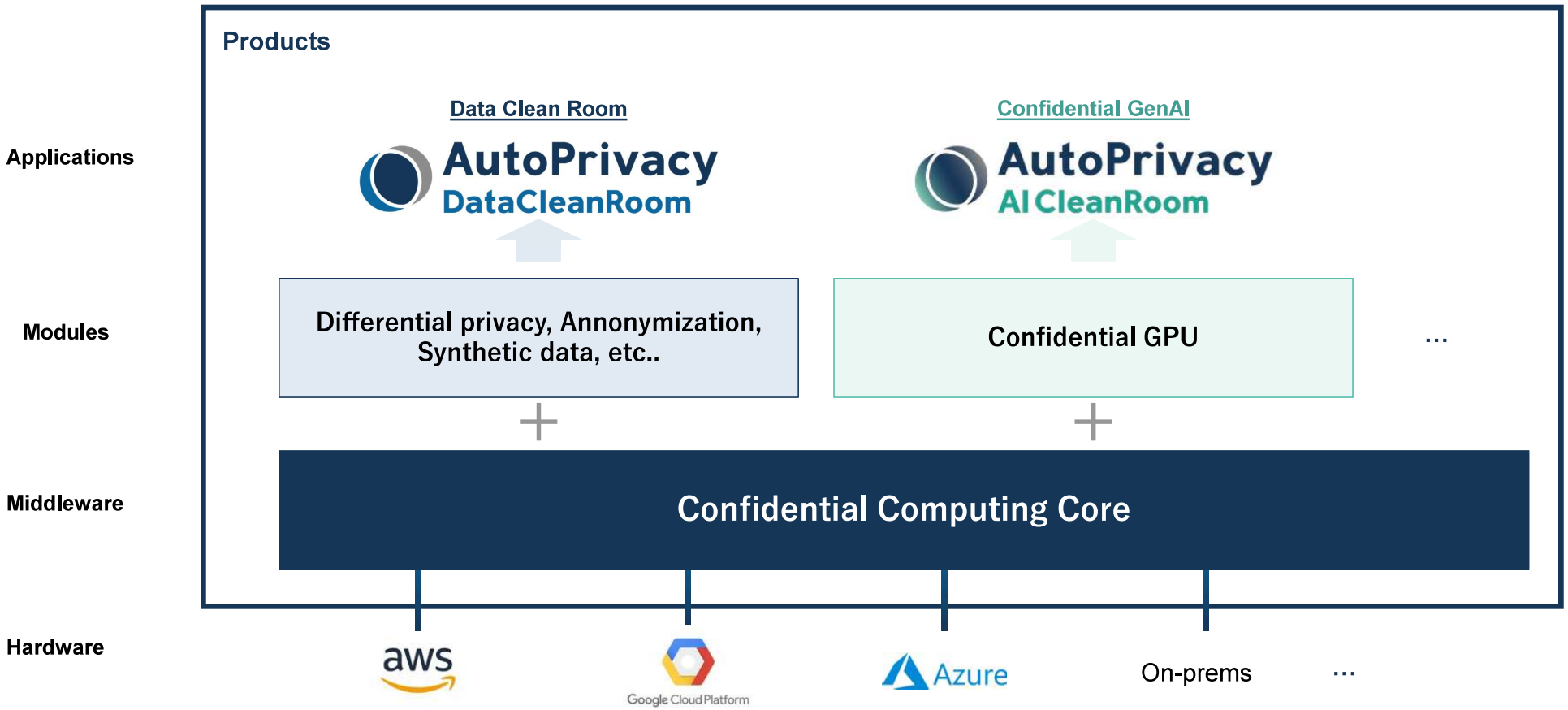
Takeharu Kondo

Co-Founder & Executive Officer

takeharu.kondo@acompany-ac.com

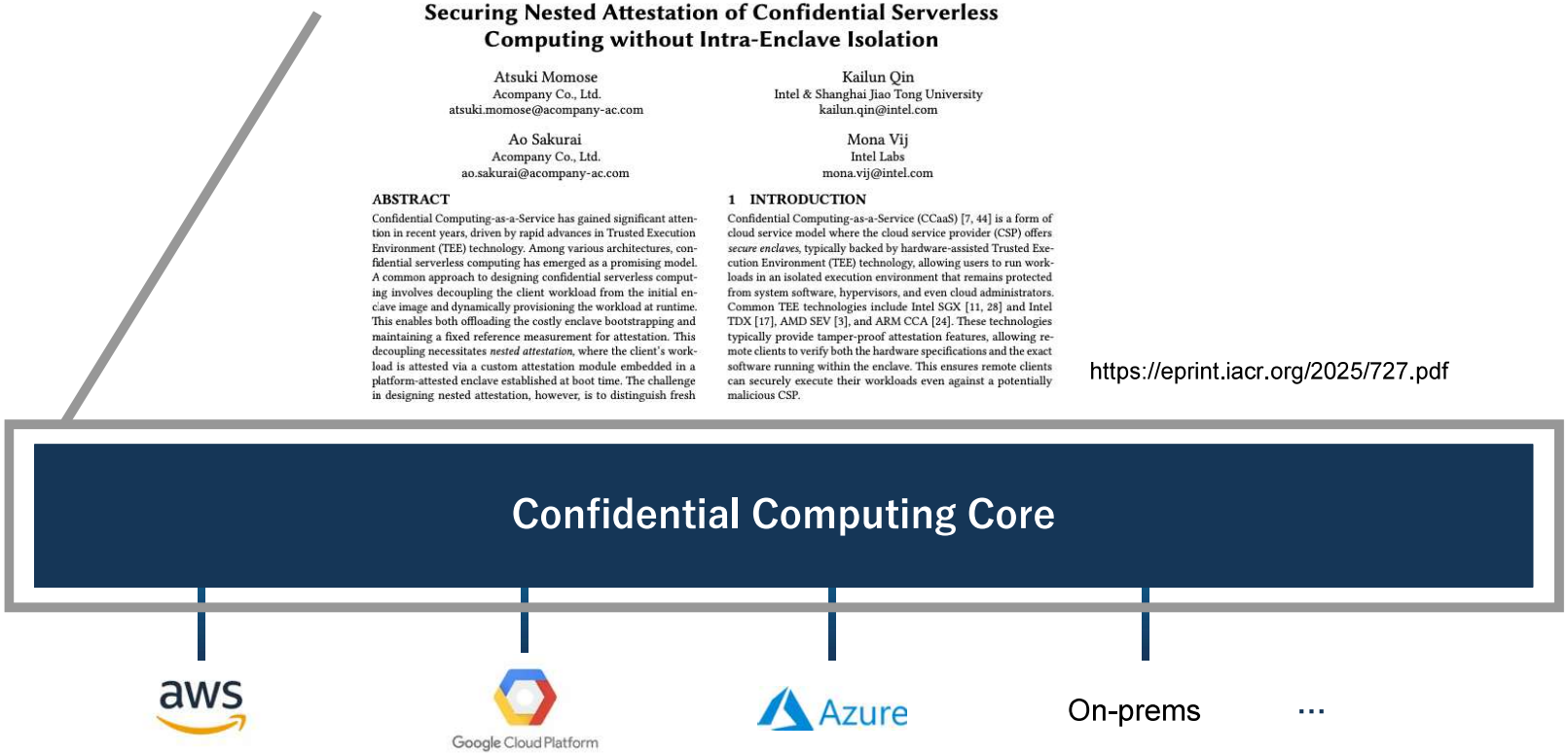
Appendix.

Provide core confidential middleware and applications



Our core technology is based on joint research with Intel

Published a joint paper with Intel(5/2025)



Securing Nested Attestation of Confidential Serverless Computing without Intra-Enclave Isolation

Atsuki Momose
Acompany Co., Ltd.
atsuki.momose@acompany-ac.com

Kailun Qin
Intel & Shanghai Jiao Tong University
kailun.qin@intel.com

Ao Sakurai
Acompany Co., Ltd.
ao.sakurai@acompany-ac.com

Mona Vij
Intel Labs
mona.vij@intel.com

ABSTRACT

Confidential Computing-as-a-Service has gained significant attention in recent years, driven by rapid advances in Trusted Execution Environment (TEE) technology. Among various architectures, confidential serverless computing has emerged as a promising model. A common approach to designing confidential serverless computing involves decoupling the client workload from the initial enclave image and dynamically provisioning the workload at runtime. This enables both offloading the costly enclave bootstrapping and maintaining a fixed reference measurement for attestation. This decoupling necessitates *nested attestation*, where the client's workload is attested via a custom attestation module embedded in a platform-attested enclave established at boot time. The challenge in designing nested attestation, however, is to distinguish fresh

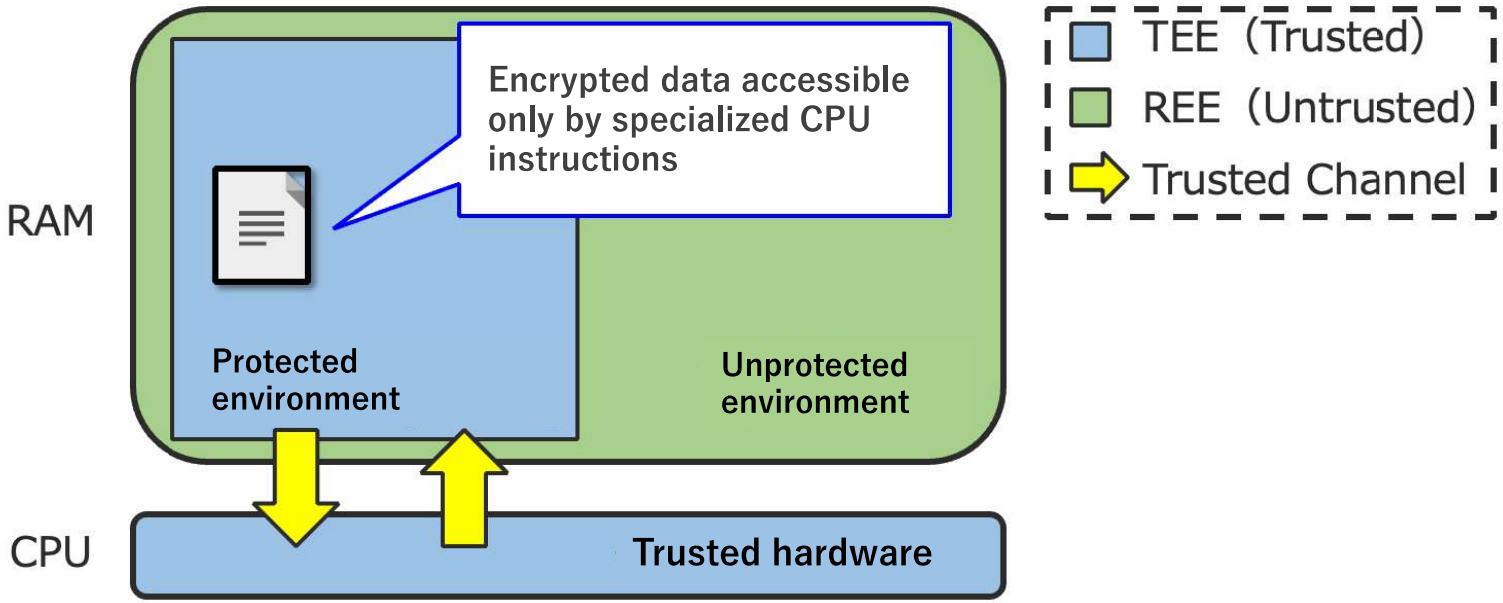
1 INTRODUCTION

Confidential Computing-as-a-Service (CCaaS) [7, 44] is a form of cloud service model where the cloud service provider (CSP) offers *secure enclaves*, typically backed by hardware-assisted Trusted Execution Environment (TEE) technology, allowing users to run workloads in an isolated execution environment that remains protected from system software, hypervisors, and even cloud administrators. Common TEE technologies include Intel SGX [11, 28] and Intel TDX [17], AMD SEV [3], and ARM CCA [24]. These technologies typically provide tamper-proof attestation features, allowing remote clients to verify both the hardware specifications and the exact software running within the enclave. This ensures remote clients can securely execute their workloads even against a potentially malicious CSP.

https://eprint.iacr.org/2025/727.pdf

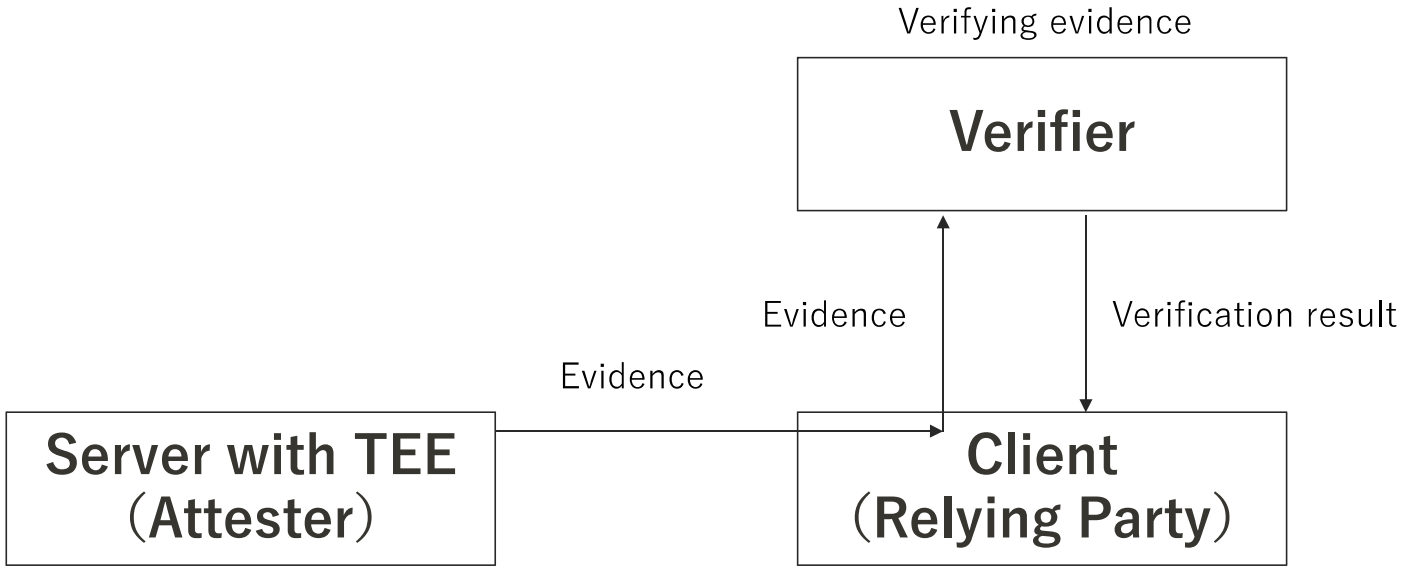
TEE is a technology that builds a protected computing environment with the support of a specialized CPU.

- Even administrators cannot access the protected environment, and plaintext data remains unseen by anyone
- Only pre-approved programs can be executed, preventing unauthorized programs from handling the data



A part of TEE technology used to verify that only pre-registered programs are executed correctly

- **Obtain evidence (e.g., hashed valued of programs) from the TEE to verify integrity**
- **Confirm that the executed program has not been tampered with**



Public Affairs Activities

- **Co-founded the Privacy Tech Association 2 years ago**
- **Leading tech and legal discussions with the government and major corporations**

Data use regulations may be eased when using Confidential Computing

日本経済新聞

AI開発向け個人情報、本人同意求めず　政府が法改正準備

経済

2025年2月11日 5:00 [会員限定記事]

保存

日経XTECH

AI開発や医療分野のデータ活用を一部同意不要に、個人情報保護委員会が法改正検討

大豆生田 崇志　日経クロステック／日経コンピュータ

2025.02.12

日本経済新聞

日本経済新聞　2025年(令和7年)2月12日(水曜日)

個人情報 AI利用しやすく

病歴や信条、同意不要に

漏洩時には課徴金

政府委案

開発促進・保護を両立

米鉄鋼関税「例外」交渉へ

トランプ氏 譲歩に「包囲網」

トランプ氏「停戦破棄」警告

ハマスに 人質全員の解放要求

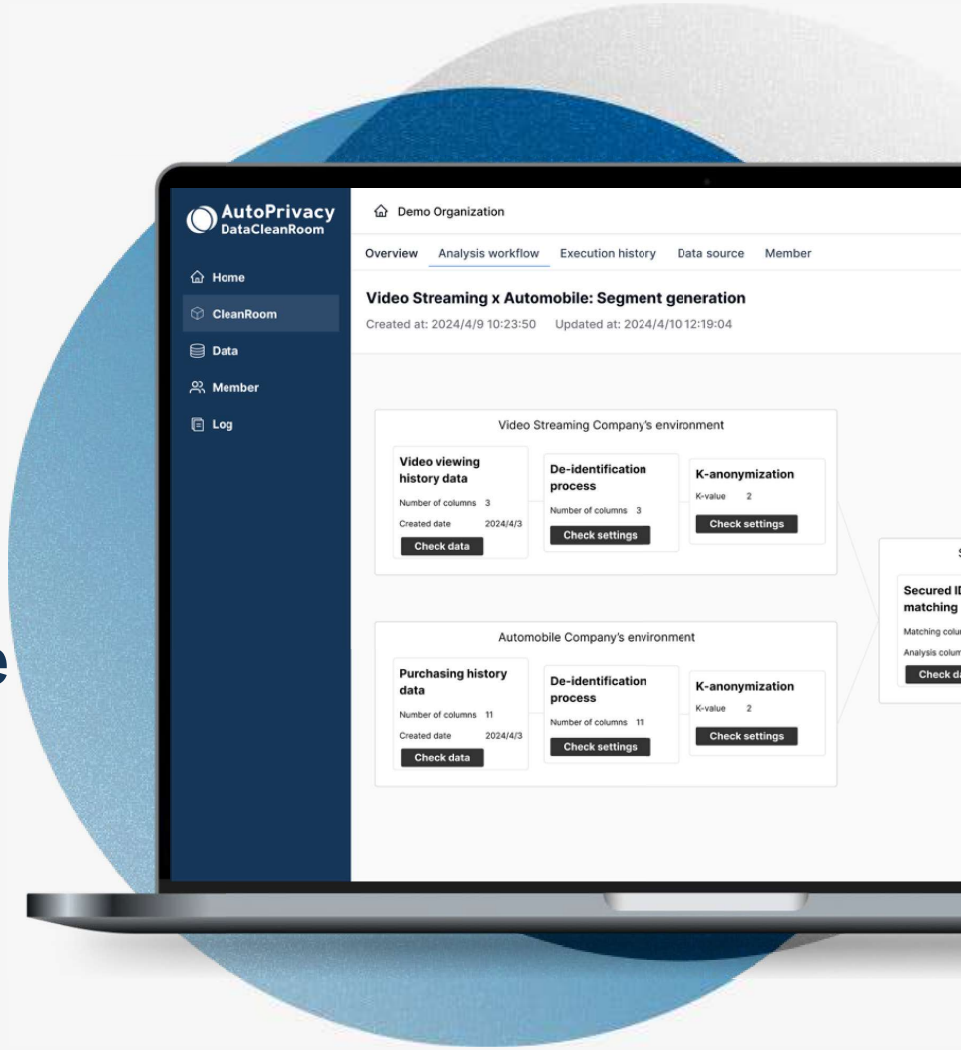
AutoPrivacy DataCleanRoom

AutoPrivacy
DataCleanRoom

Data Clean Room

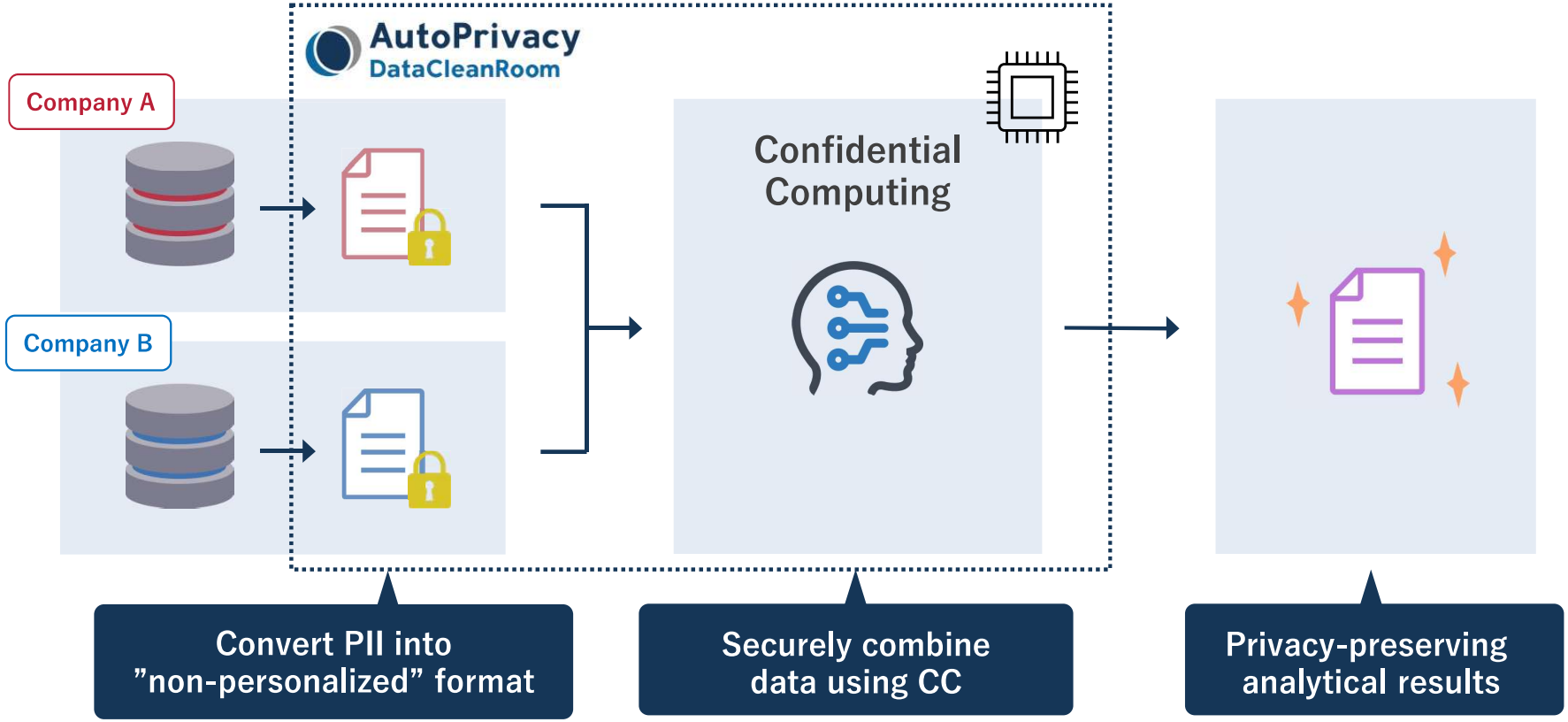
Data Collaboration with

Security & Regulatory Compliance



Product: AutoPrivacy DataCleanRoom (DCR)

Personal Data Collaboration with Security & Regulatory Compliance

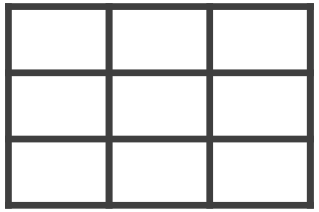


Product: AutoPrivacy DataCleanRoom

Example output of AutoPrivacy DCR

< Cross-tabulation >

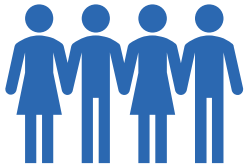
Generate cross-tabulation tables after data merging



Understand relationships and trends between attributes

< Segment extraction >

Automatically extract segments that exhibit specific trends



Identify segments that are more likely to convert

< AI models >

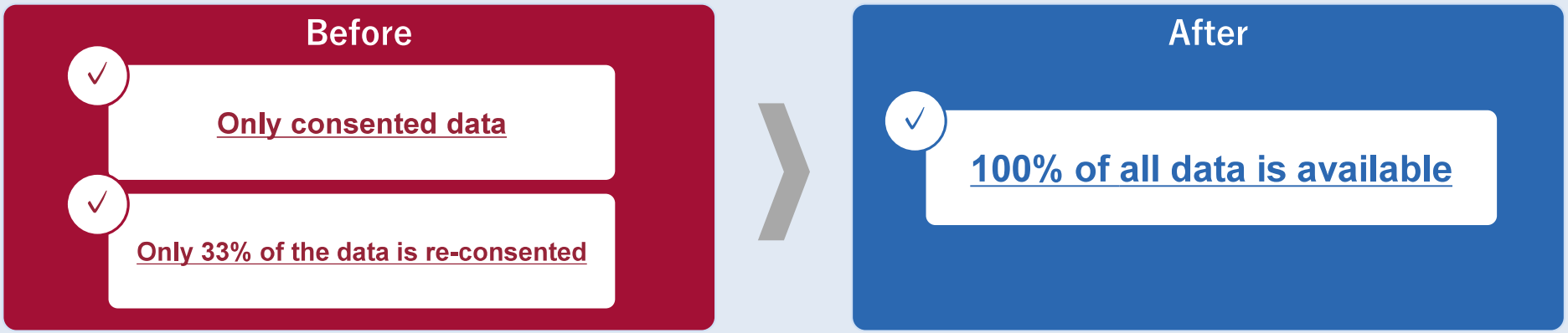
Output AI models trained on merged data

Build AI models tailored to specific use cases

Product: AutoPrivacy DataCleanRoom

All data is available without the need to re-obtain consent

In one customer case, the available data increased from 33% to 100%



AutoPrivacy DCR can connect with major cloud platforms

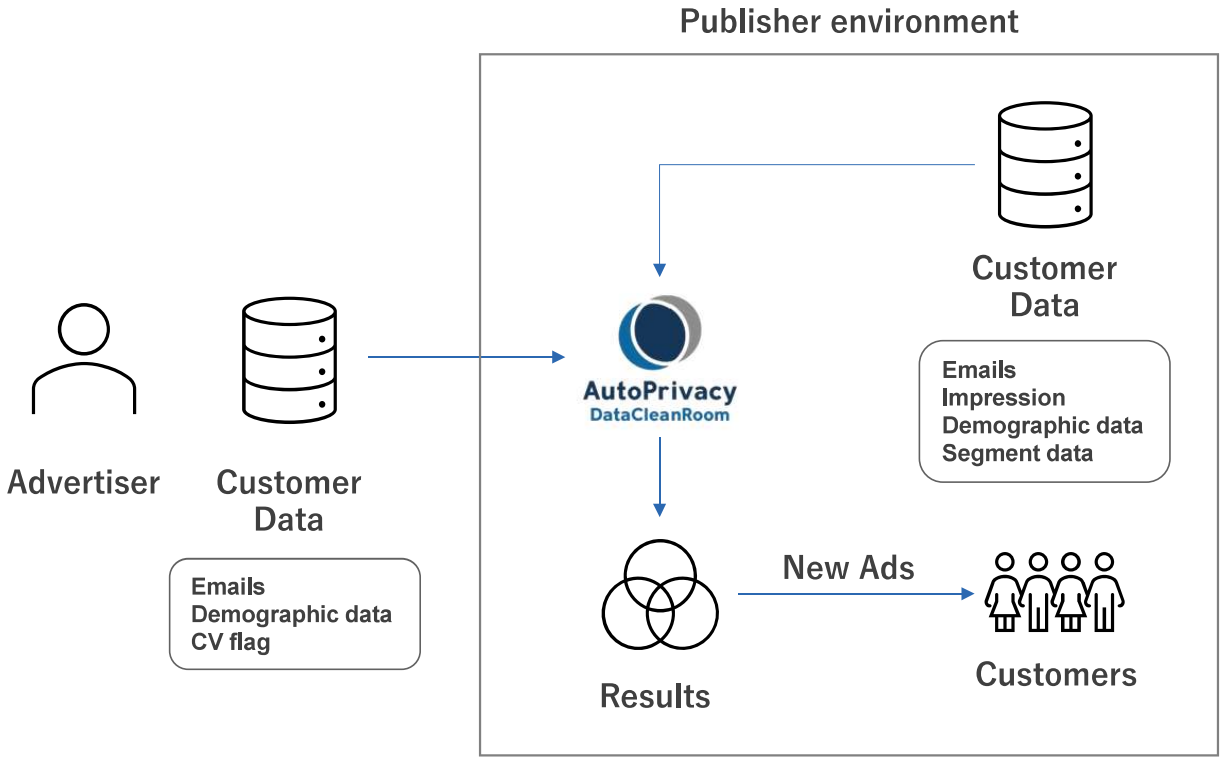
- Compatible with major cloud platforms (AWS, Azure, GCP, Snowflake), so there is no platform lock-in
- Integration with Snowflake is easiest via its Native App feature

Competitive Comparison

AutoPrivacy DCR is consent-independent and free from platform lock-in, making data integration seamless

	AutoPrivacy DataCleanRoom	Snowflake	TreasureData
Ease of installation	◎	◎	○
Regulations	◎	△	△
Consent-independent	◎	×	×
No lock-in	◎	×	◎

Combine publisher and advertiser data to measure ad effectiveness and understand customers



Measuring advertising effectiveness

Understanding customer behavior

31