CCC

COMPUTE IN CONFIDENCE.

SECURE AT EVERY LAYER.

FOSDEM

2025

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing's Recent Past, Emerging Present and Long Lasting Future

Sal Kimmich, Tech Community Architect, CCC
Feb 01 2025

CONFIDENTIAL COMPUTING CONSORTIUM

CONFIDENTIAL COMPUTING
CONSORTIUM

LINUX
FOUNDATION

Confidential Computing Consortium

- The Past: From the Secure Kernel to Confidential Compute
- The Present: Remote Attestation, Confidential Containers and CVMs
- The Long Lasting Future: Realizing the Promise of Open Security for Sensitive Compute

What is the history behind Confidential Computing?

Understanding the Past

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

Massachusetts Institute of Technology
Cambridge, Massachusetts

1. **1978 - The earliest work on privacy preserving** computation by Rivest, Adleman, and Dertouzos introduced concepts central to what would later be known as Confidential Computing.
1. ***Bee Gee's Night Fever was the top song of the year.**
2. **2009** - Fully Homomorphic Encryption (FHE) achieves a breakthrough, enabling computation on encrypted data (achieved by Craig Gentry).
3. **2015** - Intel SGX launches Trusted Execution Environments (TEEs) for secure, hardware-based computation.
4. **2019** - The Linux Foundation establishes the Confidential Computing Consortium (CCC) to drive standardization and collaboration.
5. **2020s** - AMD SEV, Arm CCA, and ecosystem maturity expand Confidential Computing adoption.
6. **2024** - NVIDIA unveils CC H100 GPUs, integrating Confidential Computing into secure AI and HPC workloads.

Understanding the Past

1. **1961:** Idea of a secure kernel: Ferranti Atlas Computer: Supervisor Extracode Routines, IBM recognizes "privileged mode" in their SPREAD Report, and this is the inspiration for the shell
2. **1971** - Intel released their first chip
3. **1971** - PDP11/45 Processor Handbook adopts "kernel" to describe the more privileged mode of execution.
4. **1974** - Security kernel prototyped by MITRE
5. **1975** - AMD released a RAM chip
6. **1985** - Arm released ARM1
7. **1995** - NVidia released NV1
8. **2019** - The Linux Foundation establishes the Confidential Computing Consortium (CCC) to drive standardization and collaboration. Founding Premier Members
9. **2020s** - AMD SEV, Arm CCA, and ecosystem maturity expand Confidential Computing adoption.
10. **2024** - NVIDIA unveils CC H100 GPUs, integrating Confidential Computing into secure AI and HPC workloads.
11. **2015** - Intel SGX launches Trusted Execution Environments (TEEs) for secure, hardware-based computation.
12. **2019** - The Linux Foundation establishes the Confidential Computing Consortium (CCC) to drive standardization and collaboration.
13. **2020s** - AMD SEV, Arm CCA, and ecosystem maturity expand Confidential Computing adoption.
14. **2024** - NVIDIA unveils CC H100 GPUs, integrating Confidential Computing into secure AI and HPC workloads.

History of Secure Kernel(s)

1. **Based on Predicate Calculus**: Secure kernels are based on **mathematical proofs**, ensuring security isn't just theoretical but **methodologically built**.
2. **Observes an Objects & Subjects Model**: The first formalized security models defined:
   - **Objects**: Resources being accessed.
   - **Subjects**: Entities with **clearance** to modify/access objects.
   - **Execution Rules**: Formal constraints ensuring security in execution

KSOS (Kernelized Secure Operating System) (1970s)

- Among the first security-focused kernels, emphasizing **formal verification**.
- **Uniquely NOT classified**: Source code was **publicly available**, rejecting "security through obscurity."

A1-Class Security Kernels (1980s)

- Defined under **TCSEC's A1-level criteria** (highest level of security).
- Designed to be **secure even if attackers have full source code**.

Final Thoughts on the Past

Foundation in Secure Kernels:

- Secure kernels utilize formal verification methods to ensure integrity and security

Advancement to Confidential Computing:

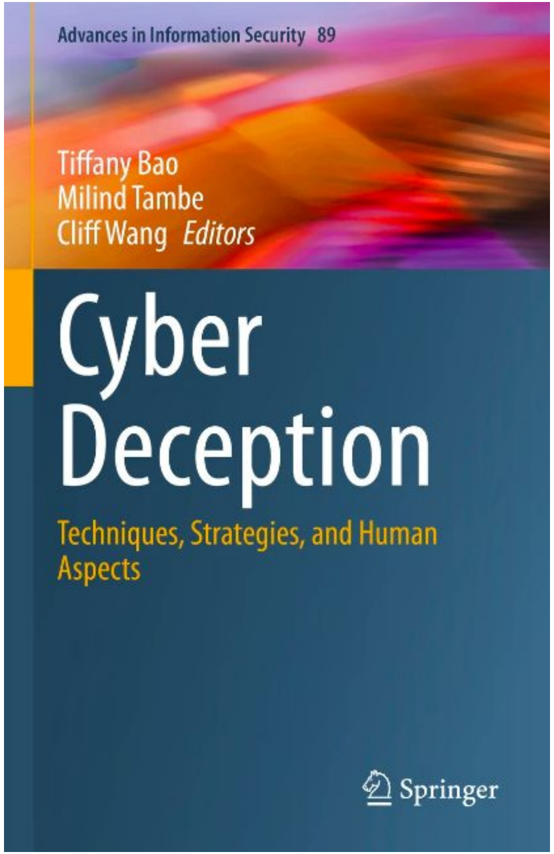
- CC extends the principles of secure kernels by creating Trusted Execution Environments (TEEs) that protect data during processing.
- This approach ensures that sensitive computations remain isolated from the underlying platform OS and other privileged software.
- Confidential Computing in Linux for x86 virtualization is a great overview

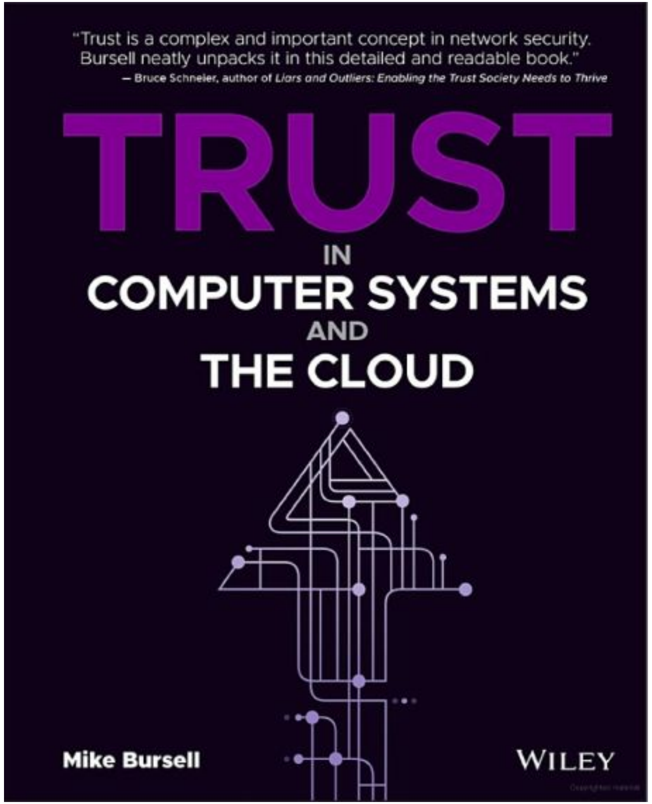
Redefined Threat Model:

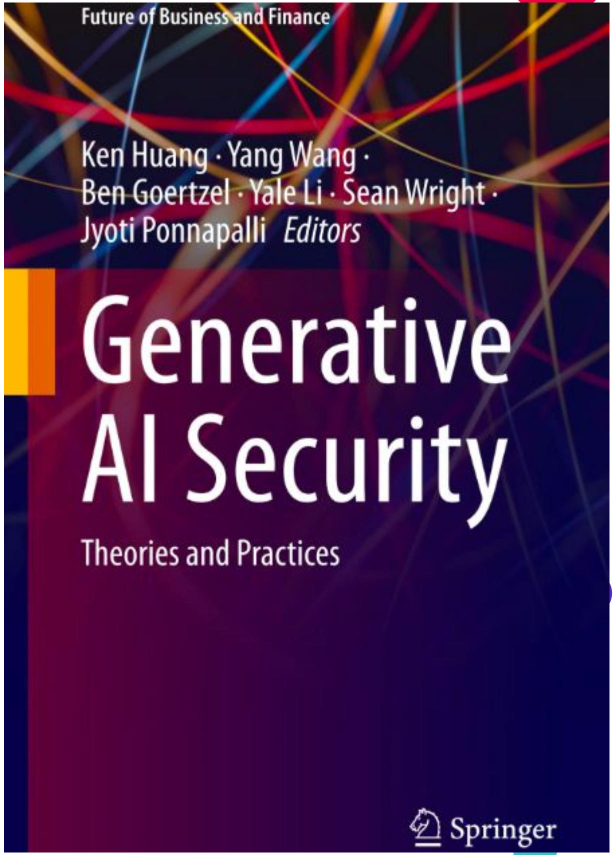
- Traditional security models often include the platform OS within the Trusted Computing Base (TCB).
- CC redefines this model by excluding the platform OS from the TCB, thereby reducing the attack surface and enhancing security.

For a long time, I’ve been figuring out how we do **security for systems with a human in the loop**.

Now, I am interested in how we do **security in a system to prevent a human, or machine, or workload identity in the loop**.







› The Present: What is the highest order **threat** are we preventing with confidential computing?

Risk of Re-Identification

"**Although anonymous data are not considered personal data**, recent research has shown how individuals can often be re-identified. Scholars have argued that previous findings apply only to small-scale datasets and that privacy is preserved in large-scale datasets. *Using 3 months of location data*, we (1) show the risk of re-identification to decrease slowly with dataset size, (2) approximate this decrease with a simple model taking into account three population-wide marginal distributions, and (3) prove that **unicity is convex and obtain a linear lower bound**. Our estimates show that 93% of people would be uniquely identified in a dataset of 60M people using four points of auxiliary information, with a lower bound at 22%. This lower bound increases to 87% when five points are available. **Taken together, our results show how the privacy of individuals is very unlikely to be preserved even in country-scale location datasets.**"

ARTICLE · Volume 2, Issue 3, 100204, March 12, 2021 · *Open Access* Download Full Issue

The risk of re-identification remains high even in country-scale location datasets

Ali Farzanehfar · Florimond Houssiau · Yves-Alexandre de Montjoye [2]

Here’s What We Know

The attention of malicious interest onto datasets that are considered benign in isolation are more likely to be harvested because the data represents a rich interaction for a sparse vector database. It is now more important than ever, to keep them in isolation.

Although anonymous data are not considered personal data <u>at this time</u>, they can certainly be used to identify a person, or group of individuals. Privacy is trending globally towards reducing this risk, but this risk exist in three states, because…

Data exists in three states:

1. In Transit: Data traversing the network
2. At Rest: Data in storage
3. In Use: Data **being processed**

Threat Vectors that Confidential Computing Stops

1. Insider Threats During Data Analysis (Jekyll and Hyde Problem):

- **Scenario:** An employee with legitimate access to a database exports sensitive information during data analysis for unauthorized purposes.
- **CC Mitigation:** By utilizing CC, sensitive data remains encrypted even during processing. Secure enclaves ensure that data is decrypted only within a protected environment, preventing unauthorized access or extraction by insiders.

2. Compromised Applications Handling Sensitive Data:

- **Scenario:** A financial application processing transactions is compromised through a zero-day exploit, allowing attackers to access data during computation.
- **CC Mitigation:** CC isolates the execution of sensitive computations within hardware-based TEEs, ensuring that even if the application is compromised, the data being processed remains protected and inaccessible to attackers.

3. Multi-Party Data Collaboration:

- **Scenario:** Multiple organizations collaborate on a joint data analysis project, requiring sharing and processing of confidential data.
- **CC Mitigation:** CC enables secure collaborative computations by allowing data to be processed in encrypted form within secure enclaves. This ensures that each party's data remains confidential, and only the agreed-upon analysis results are shared.

Confidential Computing Consortium

- The **threat model** are we dealing with in confidential computing is big: both regulated and non-regulated industries address a shared rising threat in the interaction of benign or diffused data
- The **ManaTEE project**, which will be presented by Dayeol Lee later today, is a great example of how CC can **enable privacy-preserving analytics** while still allowing researchers to access valuable datasets.
- How does the use of **secure primitives** enable confidential computing?

Four Security Primitives involved in CC

- **Confidentiality**: Protects sensitive data from unauthorized access, even during processing, using hardware-enforced encryption.
- **Integrity**: Ensures data and code are unaltered and trustworthy during processing, with hardware detecting and preventing unauthorized modifications.
- **Attestation***: Verifies the trustworthiness of a computing environment by providing a secure report on its state and configuration.
- **Hardware Root of Trust**: A foundational, immutable hardware component that anchors security operations like encryption, secure boot, and system trust verification.
  - This DevRoom used to be called **Hardware Aided Trusted Execution Environments**

Remote Attestation in Confidential Computing

Remote attestation is a security mechanism used to verify the **trustworthiness of a remote system's runtime state**. It ensures that the system is operating securely and meets predefined security requirements before it is trusted to process sensitive data or workloads.

Key Focus of Remote Attestation:

- **Runtime Verification**: Ensures that the current state of a system (hardware, firmware, and software) aligns with security baselines.
- **Evidence-Based Trust**: Uses cryptographic evidence (e.g., measurements or claims) from the system being evaluated (the **Attester**) to provide assurance.
- **Dynamic Security**: Provides real-time or near-real-time validation of a system's security posture, allowing decisions to be made dynamically based on trust.
- **Secure Communication**: Ensures the evidence exchanged is authentic, untampered, and transmitted securely.

Remote Attestation in Confidential Computing

Remote attestation is a security mechanism used to verify the **trustworthiness of a remote system's runtime state**. It ensures that the system is operating securely and meets predefined security requirements before it is trusted to process sensitive data or workloads.

How I explain this to a lawyer, compliance officer or potential adopter:

“Attestation gives organizational endorsements of "proper governance" by showing measurements are expected by infrastructure.”

Balancing Authentication and Attestation

Authentication: Validates the identity of an entity (e.g., a user or device) in a communication process.

Attestation: Provides evidence about the system's state, ensuring it operates in a trusted environment.

a. **Attestation Key (AK):** Used to generate evidence of the system's integrity and trustworthiness.

b. **TLS Identity Key (TIK):** Utilized in Transport Layer Security (TLS) protocols to establish secure communication channels.
   i. **Ephemeral Keys:** Short-lived keys that enhance security by reducing the risk of key compromise.
   ii. **Long-Term Keys:** Persistent keys that provide consistent identity verification over time.

Protocol Integration: Ensure that attestation mechanisms are integrated into communication protocols without replacing traditional authentication methods.

Balancing Authentication and Attestation

	Authentication	**Attestation**
Purpose	Confirms **who** is making a request	Confirms **where & how** a request is made
Example	Passwords, certificates, biometrics	Remote attestation of hardware/software state
Key Mechanism	Identity verification (e.g., TLS)	Secure enclave verification (e.g. TEE)

Balancing Authentication and Attestation

Authentication: Validates the identity of an entity (e.g., a user or device) in a communication process.

Attestation: Provides evidence about the system's state, ensuring it operates in a trusted environment.

Key Resources to Learn More:

1. Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
2. Device Attestation Model in Confidential Computing (Intel)
3. **Attestation DevRoom Tomorrow:** https://fosdem.org/2025/schedule/track/attestation/

Balancing Authentication and Attestation

Attestation is one of the most critical primitives in CC because it ensures workloads run securely.

But what about attestation in **web environments**?

Later today, Yoshimichi Nakatsuka will be presenting **RA-WEBs**, a new approach to making remote attestation more accessible for web services, perfect for those curious about **browser compatibility for CC**.

Session @ 13:10: *RA-WEBs: Remote Attestation for Web Services*

Secure Primitives in Confidential Compute

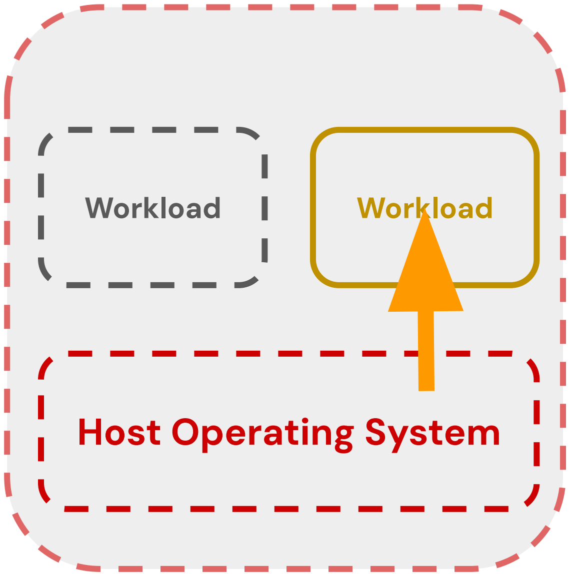
Secure primitives ensure that the building blocks—such as **attestation, encryption, and secure storage**—are in place to support **trusted execution** and **secure data management**.

CCC Example: **Keystone** uses TPM-based primitives to continuously verify runtime integrity on Linux-based systems (RISC V), illustrating how confidential computing extends the **secure Linux kernel architecture** into the cloud.

Workloads and host

Standard virtualization model

→ Type 1 - workload from workload isolation
  → VMs and containers handle this pretty well
→ Type 2 - host from workload isolation
  → VMs and containers handle this pretty well
→ Type 3 - workload from host isolation
  → VMs and containers don't handle this

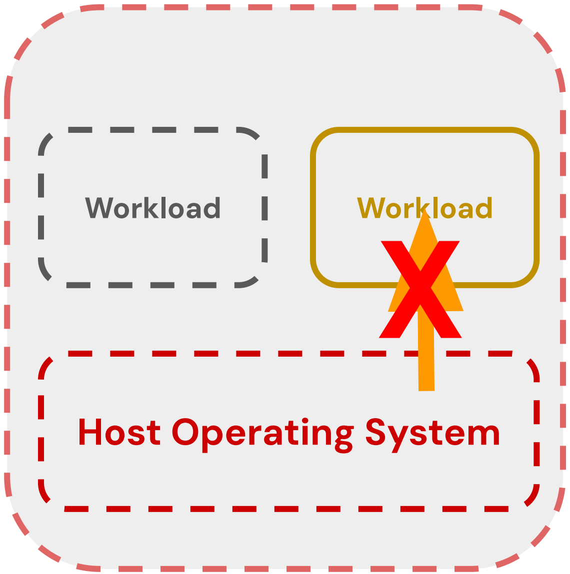


Trusted Execution Environments

Type 3 isolation is very important for many cloud-native workloads:

→ Sensitive data
→ Sensitive applications

Hardware-based TEEs provide type 3 isolation (and also types 1 & 2)



What is Confidential Computing?

Confidential Computing is

"... the protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment."

Confidential Virtual Machines

Confidential Computing: It's about protecting sensitive application code and data within Trusted Execution Environments

Confidential Computing with CVMs: The emphasis is on providing a secure, isolated VM that can run applications in a protected environment, leveraging the hypervisor and hardware capabilities.

CVMs and Secure Workloads

We've seen a major shift from traditional TEEs to full Confidential Virtual Machines (CVMs).

CVMs leverage **AMD SEV-SNP** and **Intel TDX**

Key challenges: Secure boot, measured boot, attestation, memory encryption

Find out more in the **Next Session @ 11:05**: *Confidential Virtual Machines Demystified* (Ankita Pareek & Archana Choudhary)

Confidential Containers

CoCo (Confidential Containers): Extend confidential computing principles to containerized applications, providing an additional layer of security for deploying applications across various cloud environments.

Confidential Containers ensure containerized workloads can be run in a secure and isolated manner, leveraging TEEs (Trusted Execution Environments) to **protect data in use**.

Slide from Ijlal Loutfi's (Canonical) Confidential Computing Demystified

Confidential Containers

A big part of Confidential Computing adoption is making it **seamless for cloud-native workloads**. The **Confidential Containers (CoCo) project**, which Aurélien Bombo will be covering later today, tackles exactly that—bringing trusted execution to Kubernetes with secure storage.

Session @ 12:45: *Trust No One: Secure Storage with CoCo*

What are the most compelling use cases right now?

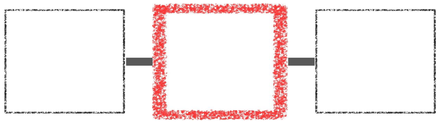
Categorisation of CCC OS Projects

Contextual Use:

- **Cloud Environments**: Intel SGX, AMD SEV used for public and hybrid cloud workloads.
- **Mobile & IoT**: ARM CCA for on-device computing, AI, and secure messaging.
- **Distributed Systems**: Multi-party frameworks like Veracruz for secure data sharing and collaboration.

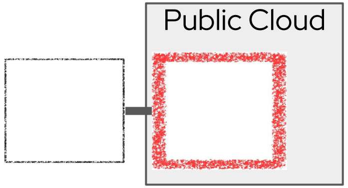
Categorisation of Use Cases

Partner Interaction



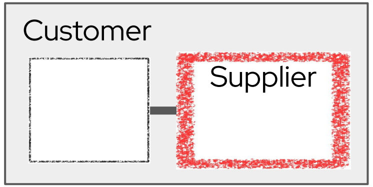
2 protected datasets interacting in confidential container

Secure Cloudburst



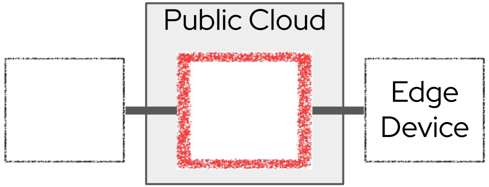
Using the public cloud to for peak workload or shared resources

IP Protection/Integrity



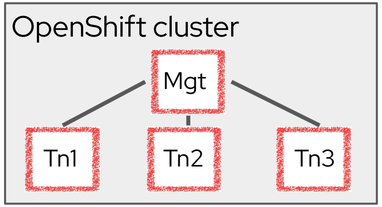
Protection of supplier data and business logic in customer environments

Edge use case



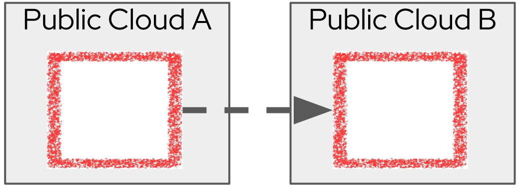
Protecting Edge device data in the public cloud for aggregation

Total Tenant Isolation



Isolating OpenShift Tenants

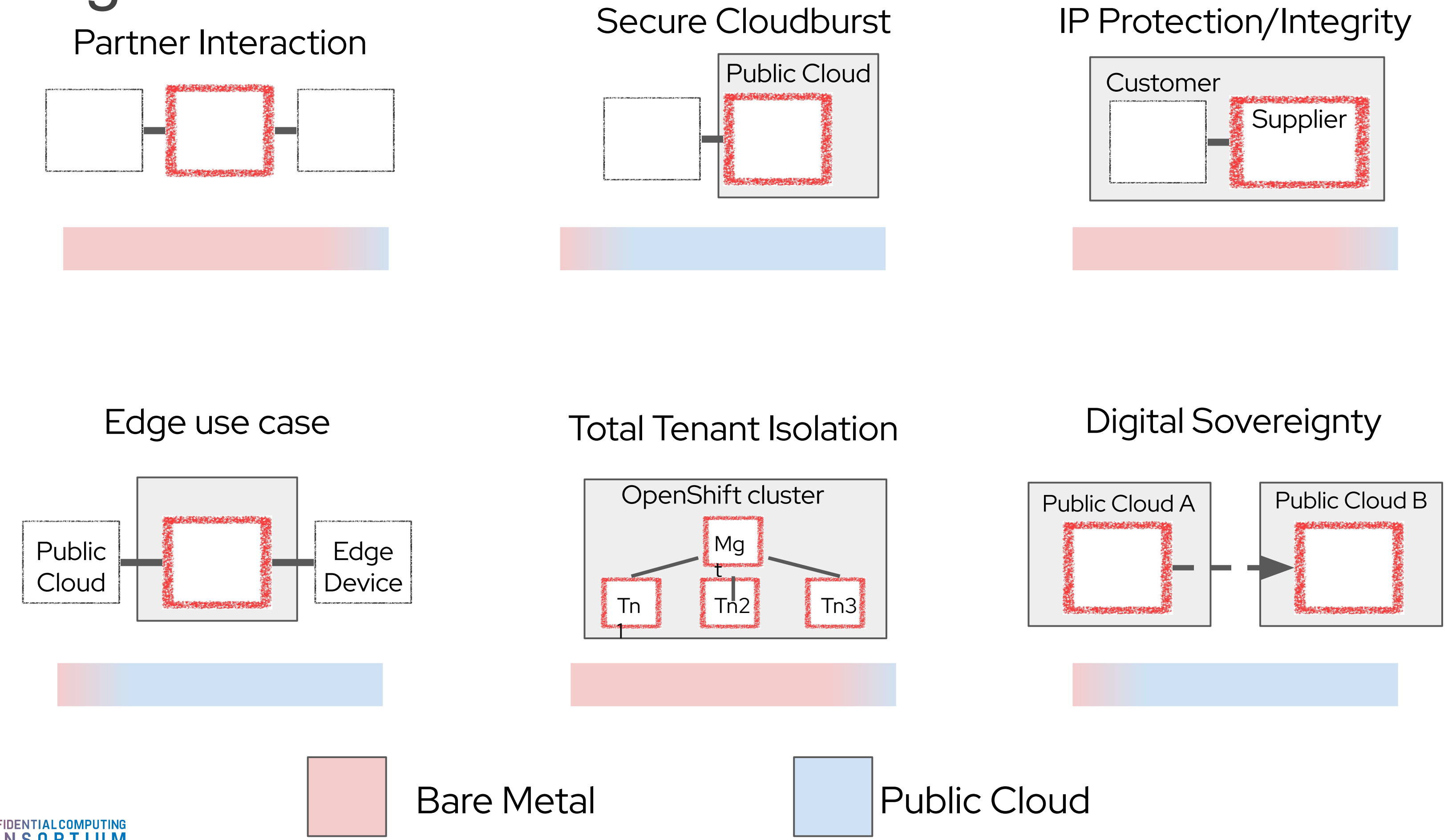
Digital Sovereignty



Encapsulating and moving workload from one provider to the next.

CONFIDENTIAL COMPUTING CONSORTIUM

Categorisation of Use Cases



CONFIDENTIAL COMPUTING CONSORTIUM

Slide from Axel Saß (RedCat) Confidential Computing: A Use Case Mini Session

Confidential Computing for Human Rights

- When fighting modern slavery, Intel technology enables the Private Data Exchange to leverage Confidential Computing, which processes sensitive data out of view from unauthorized software or system administrators.
  - Organizations like Hope for Justice and Slave-FreeAlliance have joined the effort to find victims, as well as perpetrators. The Private Data Exchange is a innovative project in partnership with Intel and Edgeless, to develop a platform to protect sensitive information
  - This project enables multiple global organizations to collaborate and share analyses to prevent human trafficking, and respond to situations of exploitation, and ensure victims receive the support they need while shielding their confidential information or regulated data.

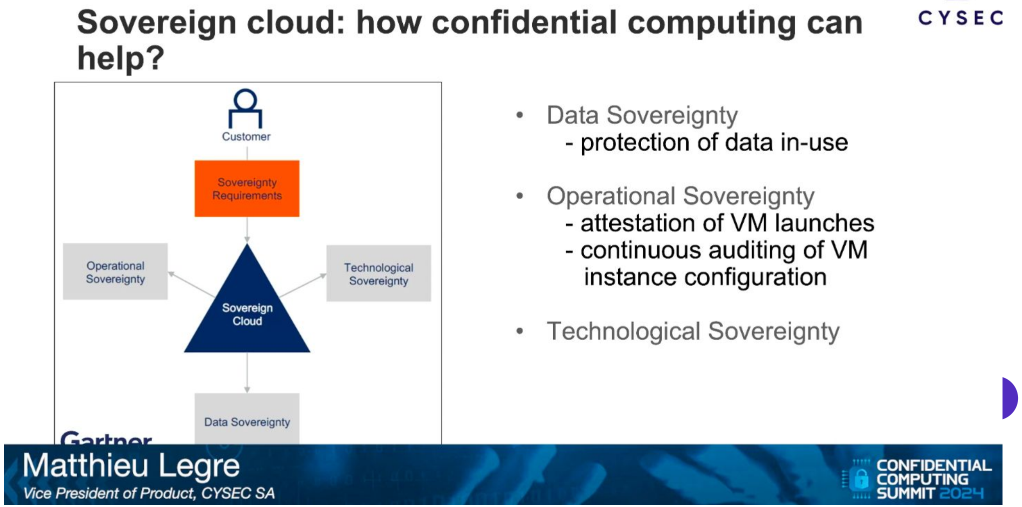
Private Data Exchange – Leveraging Confidential Computing to Combat Human Trafficking and Modern Slavery

Sovereign Cloud between Italy, Switzerland and France

Data Sovereignty - protection of data in use

Operational Sovereignty - user that wants transparency to host operations

- Attestation of VM launches
- Continuous auditing of VM instance configuration
- Extend supervision they have on their VM to some operations of the host related to isolation agreed to between two parties



CYSEC

[Sovereign Private Cloud: A Confidential Computing Solution for the Italian Public Administration]

How does regulation impact the present moment?

Regulation: Digital Operational Resilience Act

What is DORA?

- Strengthens **financial ICT resilience** across the EU.
- Applies to **banks, insurers, and investment firms**.
- **Enforcement:** January 17, 2025.

Data Security (Article 8, Paragraph 2)

- Ensures **resilience, confidentiality, and integrity** of data **at rest, in transit, and in use.**

How Confidential Computing Helps:
Secures data in use - closing a key security gap.
Uses Trusted Execution Environments for isolated, protected processing.
CC Uniquely, fully aligns with DORA's security mandates for financial institutions.

Regulation Impacting Confidential Computing

Cyber Resilience Act (CRA)

- EU regulation ensuring **cybersecurity in digital products**.
- **Requires security throughout a product's lifecycle**.
- **Confidential Computing** protects **data in use** & secures execution environments.

IETF Draft: Workload Identity Use Cases

- Defines **secure workload identity** & authentication challenges.
- **CC ensures trusted environments** for sensitive workloads.

AI Controls Matrix (Cloud Security Alliance)

- Guides **secure & responsible AI development**.
- **Aligns with CC** to **enhance AI data confidentiality & integrity**.

Why Regulations Will Drive Adoption through 2027

1. **DORA** → Financial security compliance (protecting transaction data in use)
2. **CRA** → Secure lifecycle management for digital products (trusted environments for code execution)
3. **IETF** → Workload identity as a fundamental building block for CC adoption
4. **AI Controls Matrix** → Ensuring AI workloads are processed securely with Confidential Computing

The Future of CC is Now

CC adoption is exploding—major cloud providers (Azure, Google Cloud, AWS) are integrating CC **at scale**.

Regulators are watching—DORA, CRA, AI Act **are making CC a necessity**.

Zero Trust is evolving—CC is becoming the **default security model** for sensitive workloads.

This isn't just about protecting data—it's about **building a computing world where trust is built-in, not bolted on.**

The Future of CC is at FOSDEM

Arm CCA: A full-stack **Confidential Computing reference architecture**

RISC-V & Spock: A lightweight **software-based TEE** for embedded systems

Intel TDX & Mushroom: Secure Linux workloads with a **minimal TCB**

Session @ 11:55: *Supporting Confidential Computing on Arm*
Session @ 13:35: *Spock: A Software-Based RISC-V TEE*
Session @ 14:00: *Running Mushroom on Intel TDX*

Confidential Computing Consortium

- The Past: From the Secure Kernel to Confidential Compute
- The Present: Remote Attestation, Confidential Containers and CVMs
- The Long Lasting Future: Realizing the Promise of Open Security for Sensitive Compute

CONFIDENTIAL COMPUTING CONSORTIUM

LINUX FOUNDATION

Understanding Linux Foundation Special Interest Groups (SIGs)

Special Interest Groups (SIGs) within the Linux Foundation are collaborative groups that focus on specific areas of interest in the broader landscape of open-source projects and technologies. SIGs play a crucial role in fostering innovation, sharing knowledge, and working on common goals within their respective domains. Members of SIGs include industry professionals, developers, researchers, and **anyone passionate** about contributing to the advancement of open-source technologies.

SIGs in the Confidential Computing Consortium (CCC)

The Confidential Computing Consortium (CCC) supports several SIGs focused on different aspects of confidential computing. These groups work on initiatives such as developing open standards, creating reference architectures, and enhancing the security and usability of confidential computing technologies.

SIGs <u>You</u> Should Know About

Confidential Computing Developers: For more information on the cutting edge of development for CCC member technologies, we suggest joining the **Attestation SIG**

Privacy Engineers with Regulated Compute: For updates and developments in CC regulation, we suggest joining the **Governance, Risk and Compliance SIG**

confidentialcomputing.io/about/committees/

Anyone passionate can join live to any of our SIG meetings: you can simply join in on the zoom link to get involved. All CCC meetings are recorded and available for review.

For more information on all CCC member technologies in this area, join our mailing list: lists.confidentialcomputing.io/g/main/subgroups

CONFIDENTIAL COMPUTING
CONSORTIUM

LINUX
FOUNDATION

CCC

COMPUTE IN CONFIDENCE.

SECURE AT EVERY LAYER.

FOSDEM

2025

CONFIDENTIAL COMPUT
CONSORTIU