SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Confidential Computing: Protecting Data in Use

Live Webcast

June 23, 2021

10:00 am PT / 1:00 pm ET

Today's Presenters

Moderator:
Glyn Bowden
CTO, AI & Data Practice
HPE

Presenter:
Parviz Peiravi
Global CTO/Principal Engineer, Financial Services Industry Solutions
Intel

Presenter:
Paul O'Neill
Strategic Business Development, Confidential Computing
Intel

SNIA-at-a-Glance

180
industry leading organizations

2,500
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **snia.org/technical** **@SNIA**

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

SNIA Legal Notice

The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.

Member companies and individual members may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced in their entirety without modification
- The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA.

Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.

The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

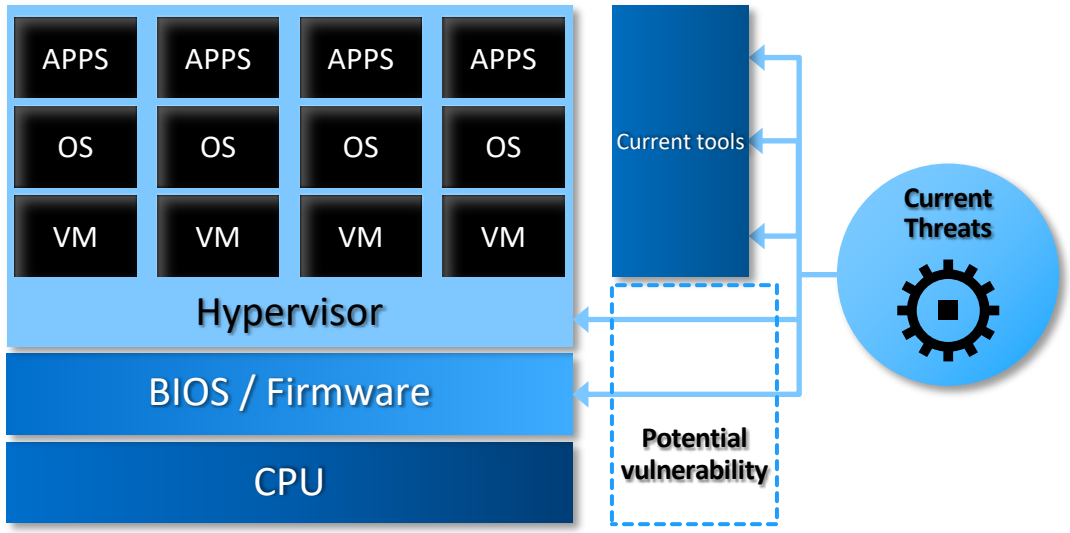
- Introductions
- Confidential Computing Overview
- What is Trusted Execution Environment (TEE) and Software Guard Extension (SGX)
- Market View of Confidential Computing
- Confidential Computing Use Cases
- Privacy Preserving Federated Machine Learning Use Case in Banking
- Key Takeaways

Overview of Data Center Security

Data Center Security Landscape

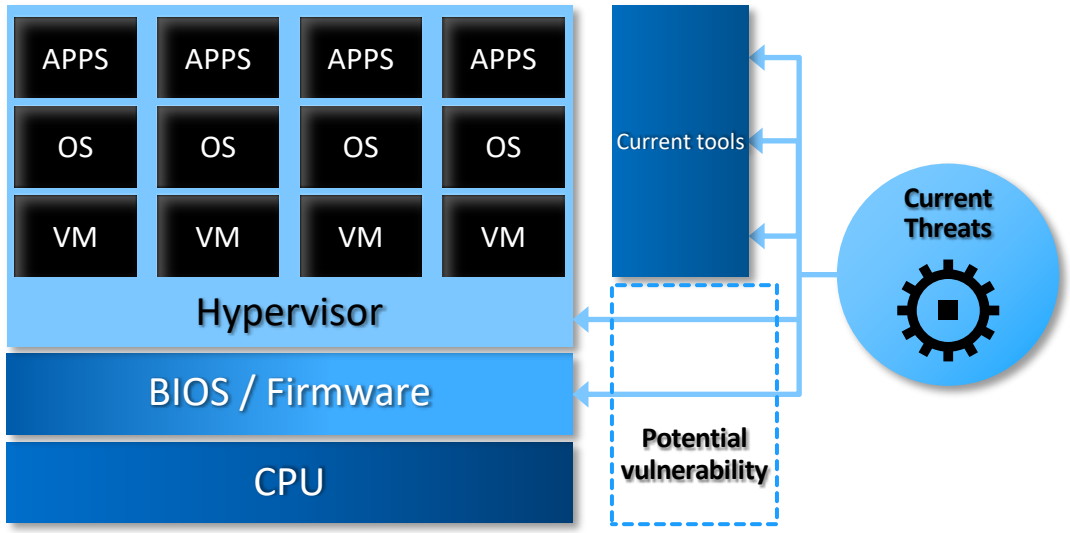
Data Center Security Strategy

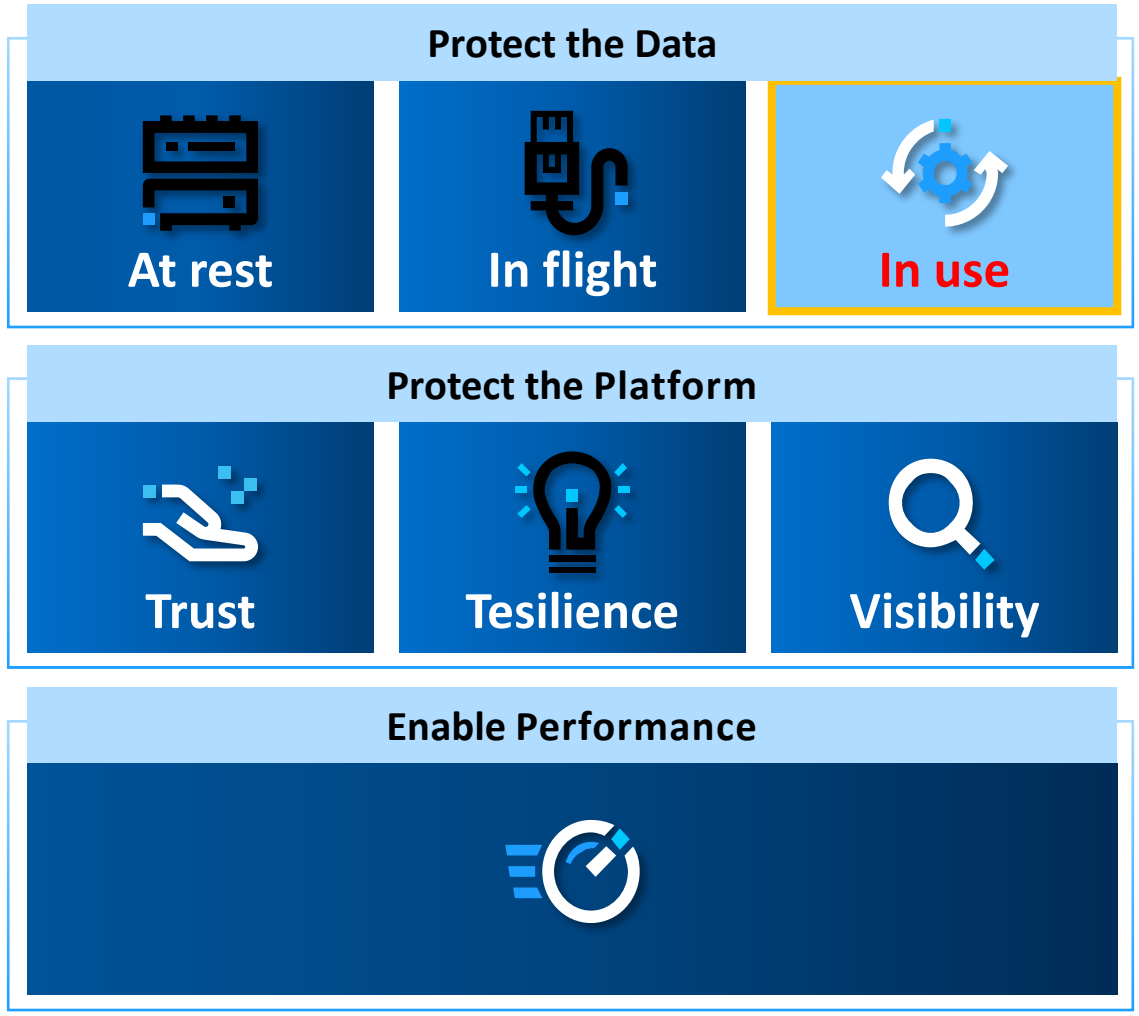
Effective security is built on a **foundation of trust.**



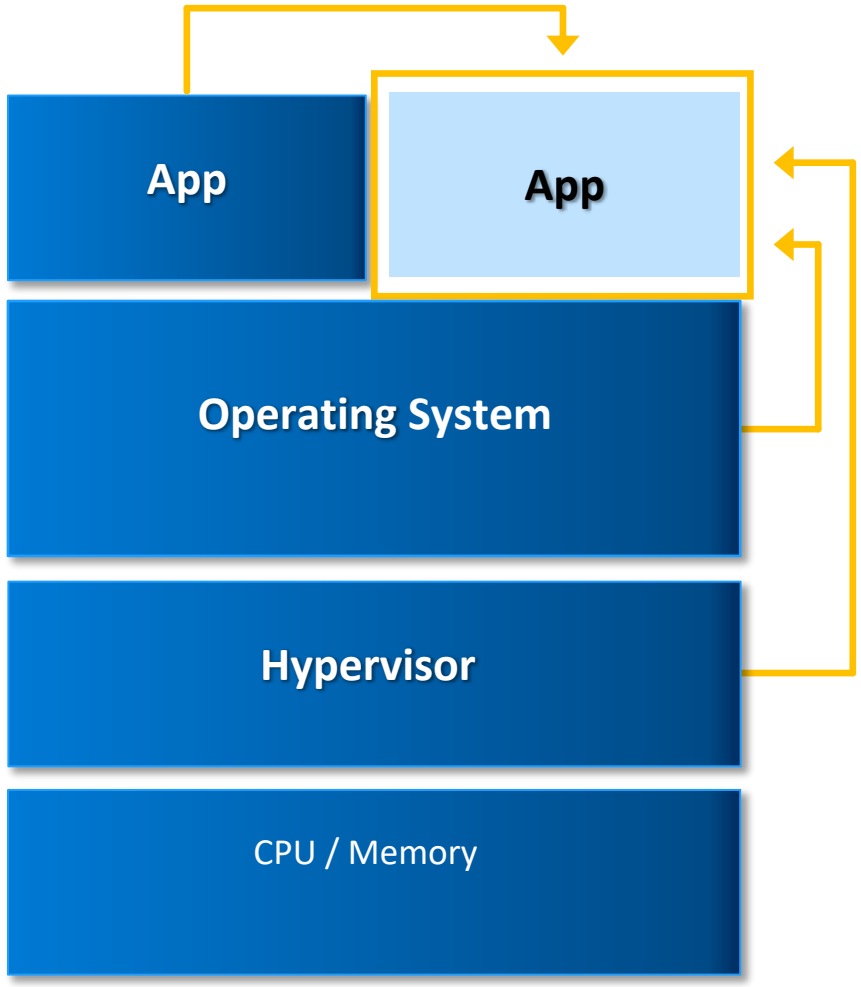
Data Center Security Strategy

Effective security is built on a **foundation of trust.**





Why Protect Data in Use?



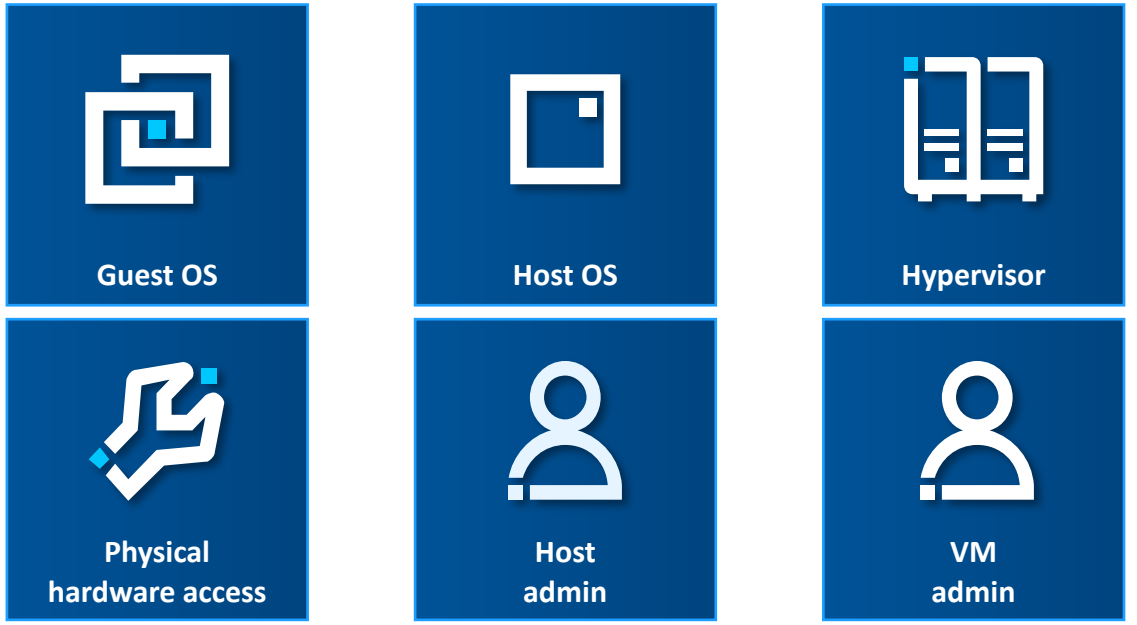
Protect against…

Malicious insiders with escalated admin privileges

Hackers exploiting bugs in the hypervisor/OS

Third parties accessing data without owner's consent

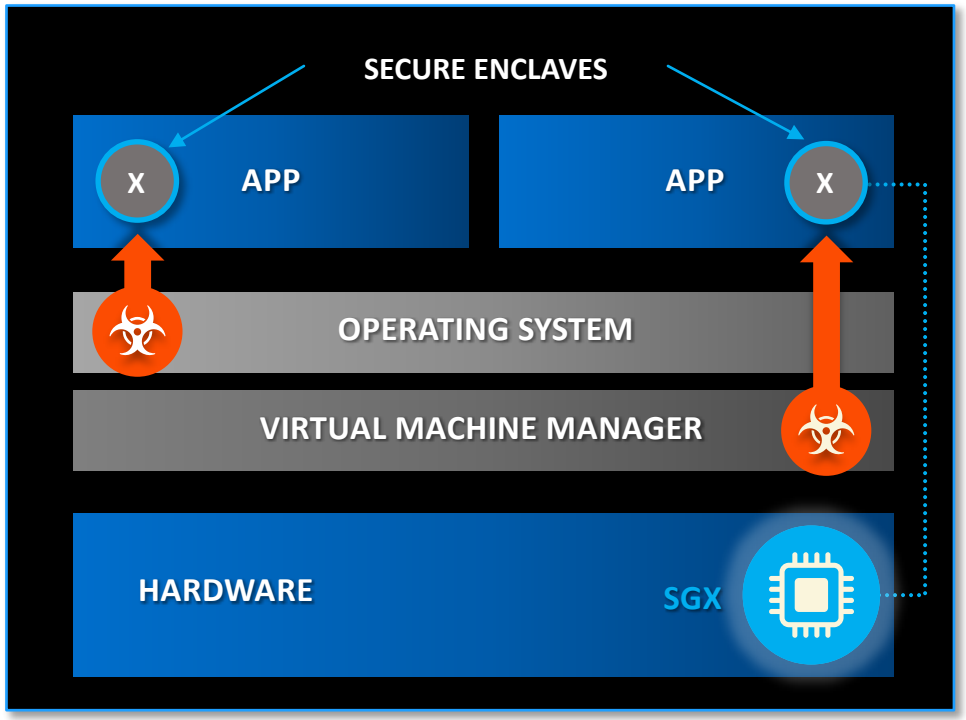
Data and Computation Exposed to…



Confidential Computing Powered by Trusted Execution Environment

Trusted Execution Environment (TEE)

Helps provide enhanced security protections for application data independent of operating system or hardware configuration.



- **Helps protect against SW attacks** even if OS/drivers/BIOS/VMM/SMM are compromised
- **Helps increase protections for secrets** (data/keys/et al) even when attacker has full control of platform
- **Helps prevent attacks**, such as memory bus snooping, memory tampering, and "cold boot" attacks against memory contents in RAM
- **Provides an option for hardware-based attestation** capabilities to measure and verify valid code and data signatures

Minimally-sized Trusted Compute Base (TCB)

Other technologies allow some privileged SW in their trust boundary

Helps enhance protections for hard-to-protect spaces

Helps increase transparency and accountability

Confidential Computing with TEE's

TEE looks to solve three key challenges:

- Execution isolation at the Trusted Execution Environment boundary → **Results in data unencrypted inside the CPU package, while data outside is encrypted and integrity checked. External snoops only see encrypted data.**
- Attestation and sealing at the Trusted Execution Environment boundary → **Hardware-based attestation provides remote assurance that the right application is executing in the right platform.**
- Recovery from hardware issues → **TCB Recovery is the process of being able to cryptographically demonstrate that the TCB has been updated to fix a potential security issue.**

Why Do We Need Confidential Computing

- Higher value workloads require security guarantees around processing:
  - Personal Identifiable Information (Privacy)
  - Government Confidential Information
  - High Value Assets
- Cloud providers already have many programs for convincing their customers, why they should be trusted?
- **Confidential Computing-based Cloud** paradigm combats rising paranoia of trusting cloud providers with customer secrets
- There are number cloud services providers offering TEE based confidential computing today

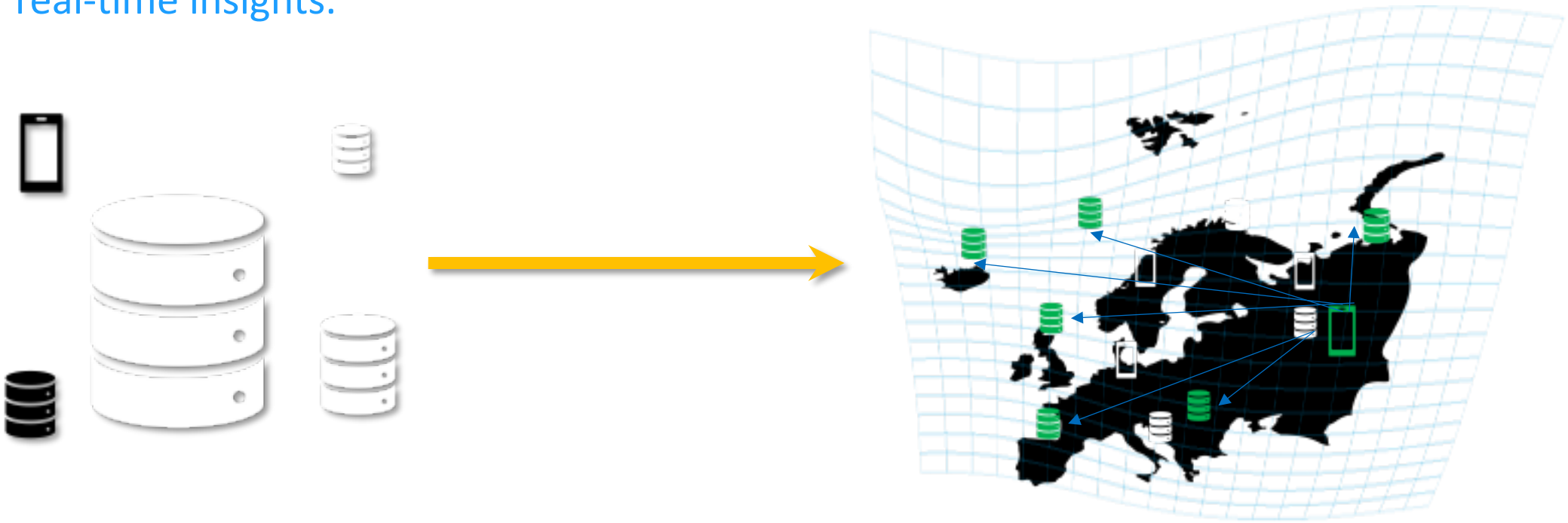
Confidential Computing Consortium Mission

- Define confidential computing and accelerate acceptance and adoption in the market
- Develop enterprise-grade building blocks (e.g. open specifications and open source licensed projects) with the latest technologies to enable easy development and management of enterprise-grade confidential compute applications
- Define foundational services and frameworks that are confidential-aware and minimize the need for trust
- https://confidentialcomputing.io/

The Confidential Computing Market is moving

A New Data Approach for Real-Time Insights

Highly regulated organizations want to move to secure, private collaborative models for real-time insights.



From Data Silos...

...to Incentivized Collaboration

By incentivizing network contributions and leveraging the progress and pace of a wide network, individual organizations will benefit more from compensated collaboration than competition.

What's the Problem with Data?

It's virtually impossible for enterprises to control how external entities process and secure their data, thus risking compliance issues .

I'm happy to share my data, I trust the Service Provider. I'm risking privacy and compliance.

Processes data

I'm not happy to share my data, I have no trust relationship with the Service Provider.

Unable to offer services processing sensitive data

"By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today" - *Gartner*[1]

1 **Gartner Predicts for the Future of Privacy 2020**

What's the Problem with Data?

What if enterprises could be sure how their data would be handled by external service providers ?

I would be happy to share this sensitive data **in encrypted form** if I know what the service provider is going to do with it.

Offers services based on processing sensitive data using TEE

Confidential Computing will help drive more data to the cloud to enable more collaboration on sensitive data, aided by hardware processor ubiquity.

Machine Learning
Multi Party Analytics
Federated Learning

Confidential Computing can help to deliver

1. Privacy of data
2. Confidentiality for cloud platforms
3. Integrity for Machine Learning

Cloud Service Provider

"By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today" - *Gartner*[1]

1 Gartner Predicts for the Future of Privacy 2020

Confidential Computing Vertical Industry Use Cases

Financial Services

- Regulatory compliance & audit
- Money laundering protection
- Asset digitalization
- Digital asset movement
- Data Analytics
- Blockchain
- Cross-border analytics

Healthcare

- Electronic health records
- Supply chain management
- Genomics
- Drug discovery
- Federated learning
- Data aggregation

Emerging

- Retail loyalty
- Supply chain
- Internet of things
- Edge compute
- Telecoms
- Industrial

Most legislated industries looking to adopt cloud economic models

Expanding Confidential Computing Usages

Cloud Infrastructure

Protect the confidentiality and integrity of customer data in-use in the multi-tenant public clouds.

Federated Learning

Enable parties to securely conduct machine learning across broader data sources while keeping algorithms and data sets confidential.

Privacy Preserving Machine Learning

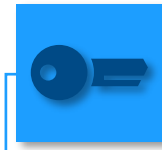
Allow collaboration between independent data owners on model training, keeping data and IP confidential.

Blockchain

Keep private data and transactions secure for authorized network participants and improve scalability capabilities.

Trusted Multi-Party Compute

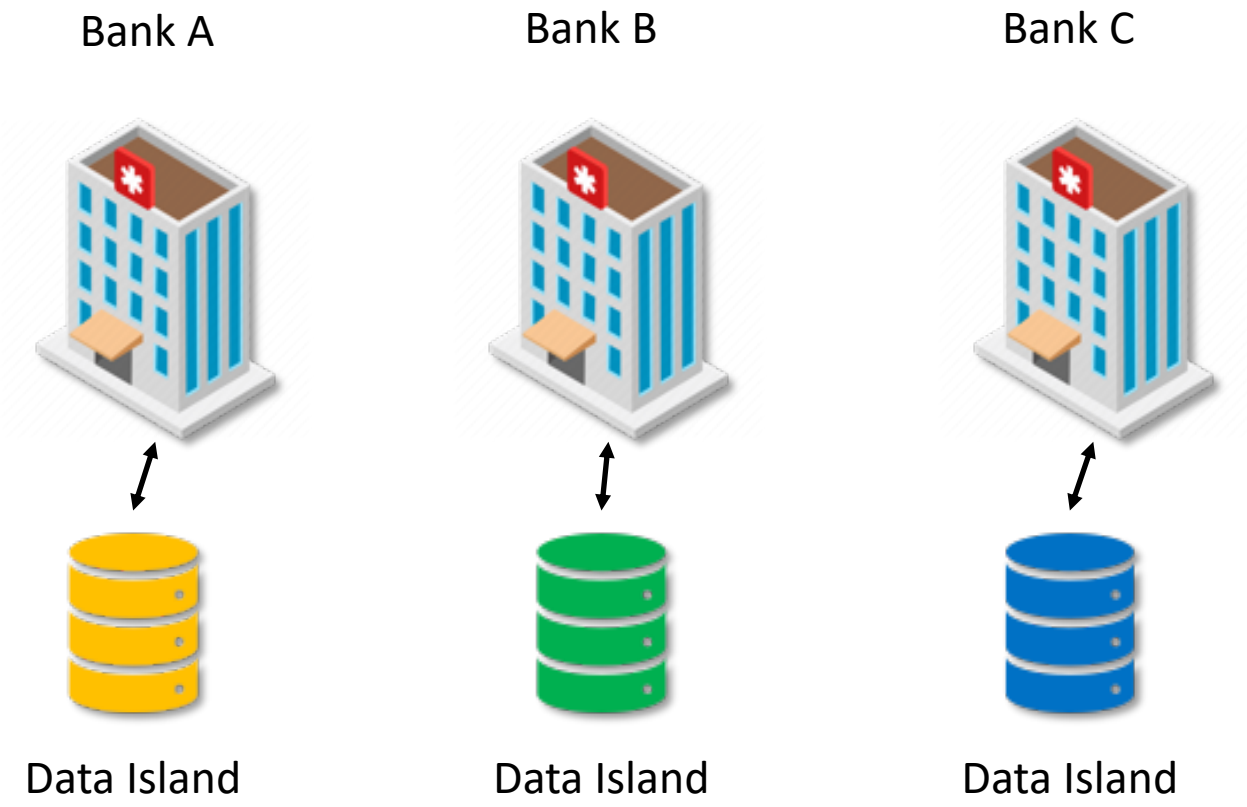
Enable multiple untrusting parties to interact on shared data while keeping sensitive data confidential.



Secure Key Management

Provide unified HSM and key management capabilities on a scalable distributed architecture.

Federated Learning



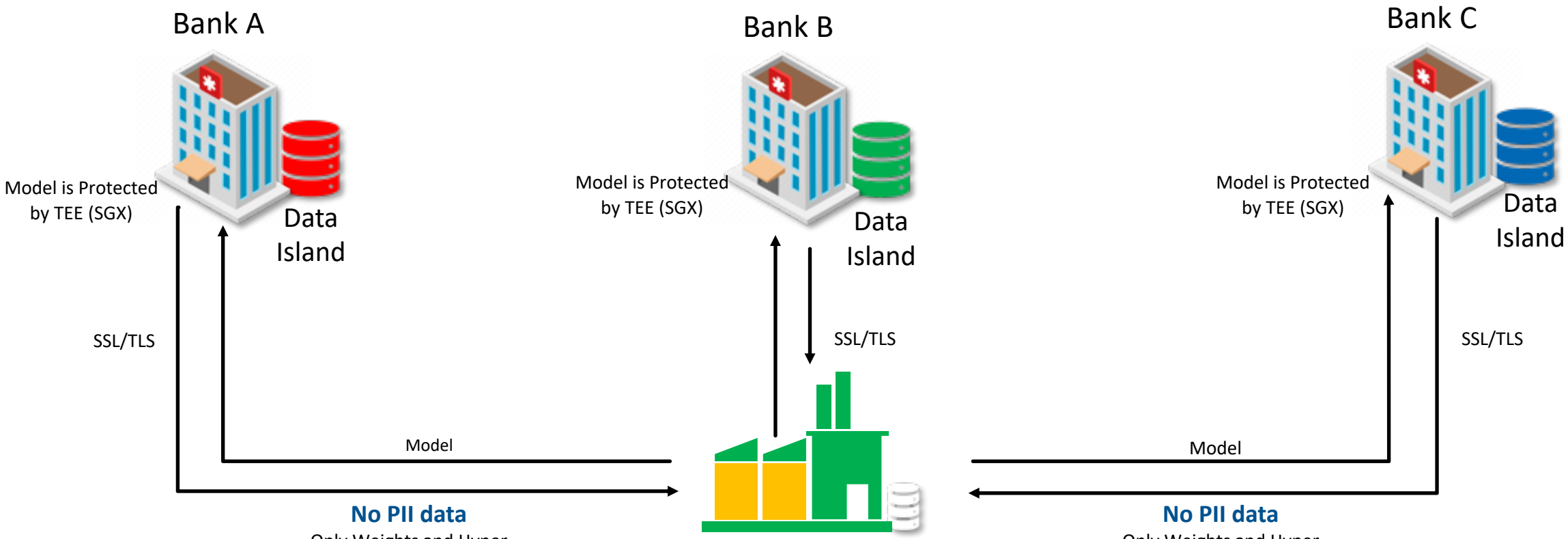
Observations

- The data in custody of every Bank forms a data island.
- Each data island has characteristics it doesn't share with other Banks.
- A model trained on data from Bank A might show poor generalization on data from a different Bank.

The conventional approach to date—to pool data from all Banks in centralized location and build a single model—presents challenges.

- Privacy and Data Sovereignty
- Data is constantly changing, meaning this pooling exercise must be repeated at ever-increasing frequencies.
- Data Gravity, Eventually data set limits are hit and no more data can be added.

Federated Learning, Centralized Model Development and Governance, Distributed Training



Privacy and Security in Federated Learning

Confidentiality

- Helps protect model IP
- Designed to prevent attacks computation
- Data is not moved, promoting privacy
- Compliance of local laws is observed

Integrity and Attestation

- Only **approved** models/training procedures
- All participants know rules are **enforced**
- Algorithmic defenses help prevent bypass

Designed to stop attackers from using the model

Designed to stop attackers from being adaptive

Building a Trusted Platform Using TEE, Key Architectural Considerations

Most control

Fastest path

New App Development

Trusted portion of applications utilize enclave for code and data

- Open Enclave (OE) SDK
- SGX SDK
- Enarx SDK
- R3 Conclave
- …more

Lift and Shift

Existing applications run natively within protected containers inside an enclave

- **Graphene**
- R3
- Fortanix
- Scone
- Edgeless Systems
- …more

Key Takeaways

- Security is foundational to business transformation
- TEE Solutions start with capabilities built in hardware
- Confidential Computing powered by TEE is fundamental to securing the most sensitive data sets in use (privacy)
- There are multiple choices in deploying TEE based solution with different levels of security offered by HW/SW/CSP vendors

Learn More! The First Session in this Series

What is Confidential Computing and Why Should I Care?

Panel Discussion with:

Mike Bursell, Co-founder, Enarx Project

David Kaplan, AMD

Ronald Perez, Intel

Jim Fister, The Decision Place

Watch on-demand: https://youtu.be/HnLfKUI0_Y4

Stay Tuned for the 3rd Webcast of this Series

Confidential Computing Use Cases

Coming in July 2021

Follow us on Twitter @SNIACloud

for date and time

Thanks for Viewing This Webcast

Please rate the webcast and provide us with feedback

This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library

A Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/

Follow us on Twitter @SNIACloud

Thank you!