SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

How to Easily Deploy Confidential Computing

Live Webcast

July 28, 2021

10:00 am PT / 1:00 pm ET

Today's Presenters

Moderator:
Michael Hoard
Storage Planning
Intel

Presenter:
Steve Van Lare
Vice President of Engineering
Anjuna Security

Presenter:
Anand Kashyap
Co-founder & CTO
Fortanix

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

- Confidential computing problem scope and vision
- Cost-effective benefits of available and easily deployable solutions
- Real-world confidential computing examples
- Confidential computing demonstrations
- Buyer's guide: things to look for in your confidential computing solution

Steve Van Lare

Vice President, Engineering

Anjuna Security

The World Runs on Secrets

…we haven't been very good at keeping them….ever.

- Israel Defense Forces Cybersecurity:
  - Keep data safe in insecure areas.
- Open DNS SaaS: Customer key existential business risks
- Stanford Research: Model exists…without real-world support
- Secure enclave technologies released creating an opportunity….

Confidently run "good guy" workloads over "bad guy" infrastructure.

Vision is to Make Confidential Compute Easy for Enterprises

- Establish a simple software construct: The Confidential Cloud
- Eliminate excess data overexposure
- Maintain app, data and IT/Business process continuity (no changes)

All the advantages of public infrastructure.

All the security of private hardware.

Everywhere!

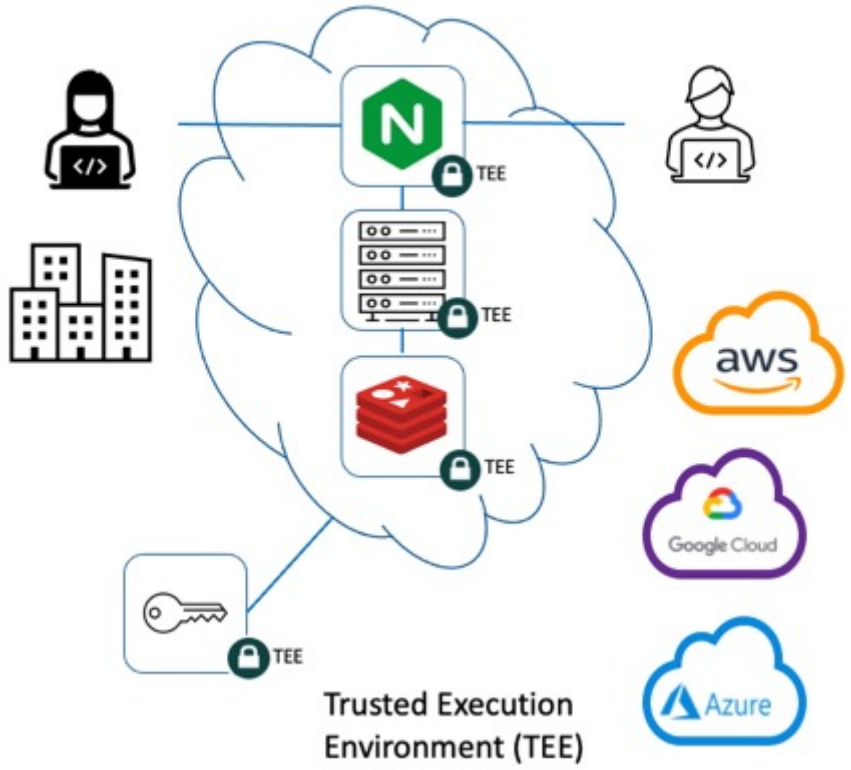
Threats Confidential Compute Protects Against

- Insiders
- External bad actors
- Malware
- Horizonal attacks
- Unauthorized Data Access
- Code Tampering
- Memory dumps

From Open to Zero Trust Computing

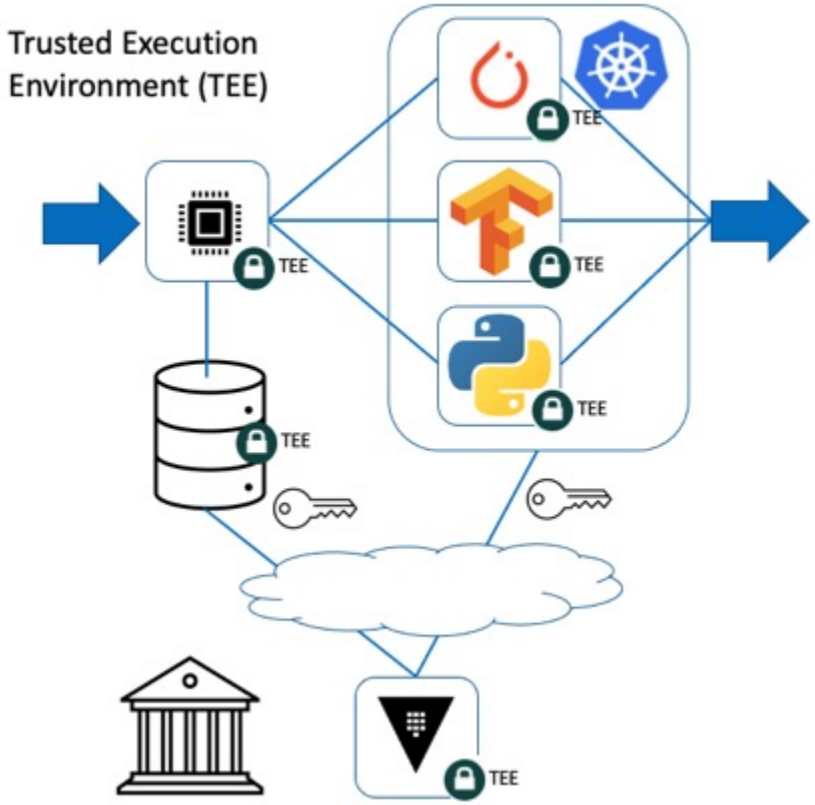
Government To Move Thousands Sensitive Applications to the Cloud

- **Opportunity**
  - Move sensitive apps to the cloud to save money on compute, infrastructure and staff.
- **Challenge**
  - Confidential Computing Technology required app rewrite and enclave tech expertise.
- **Solution**
  - Confidential Cloud establishes data perimeter around app/data/storage environment.
  - No changes to app or ops needed.
  - Leverage existing infrastructure including Key management systems.
- **Outcome**
  - Achieved simple repeatable cloud deployment, highest security and cloud-economics.
  - Pipeline of thousands of app migrations to “more secure than on site” environment.



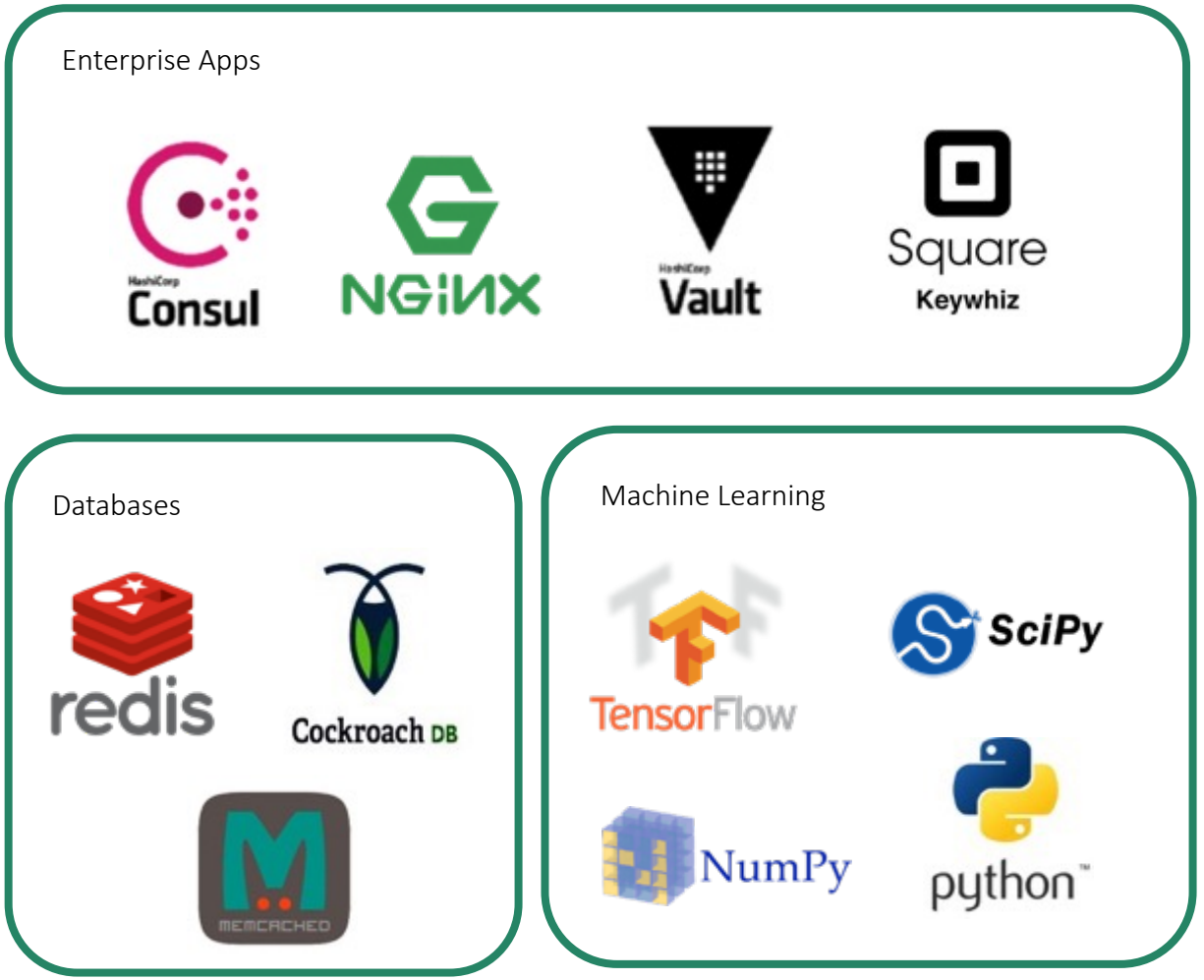
Bank Needs Hybrid Key Management and Confidential Compute Platform for Large App Portfolio

- **Opportunity**
  - App migration to hybrid cloud.
    Key management consolidation to HashiCorp hybrid
- **Challenge**
  - Secure hybrid workloads w/o HSM cost, limitations and complexity.
  - Leverage foundation for large application portfolio.
- **Solution**
  - A simple single key management solution across all clouds.
  - Confidential Cloud established as computing construct for all applications
- **Outcome**
  - Far lower cost and operational complexity with software vs. HSM. Expand beyond keys.



Zero to Confidential Cloud in 3 Minutes

1. Run an existing Redis database unprotected
2. Run in a Confidential Cloud
3. Try to breach data perimeter



Demonstration

Anand Kashyap

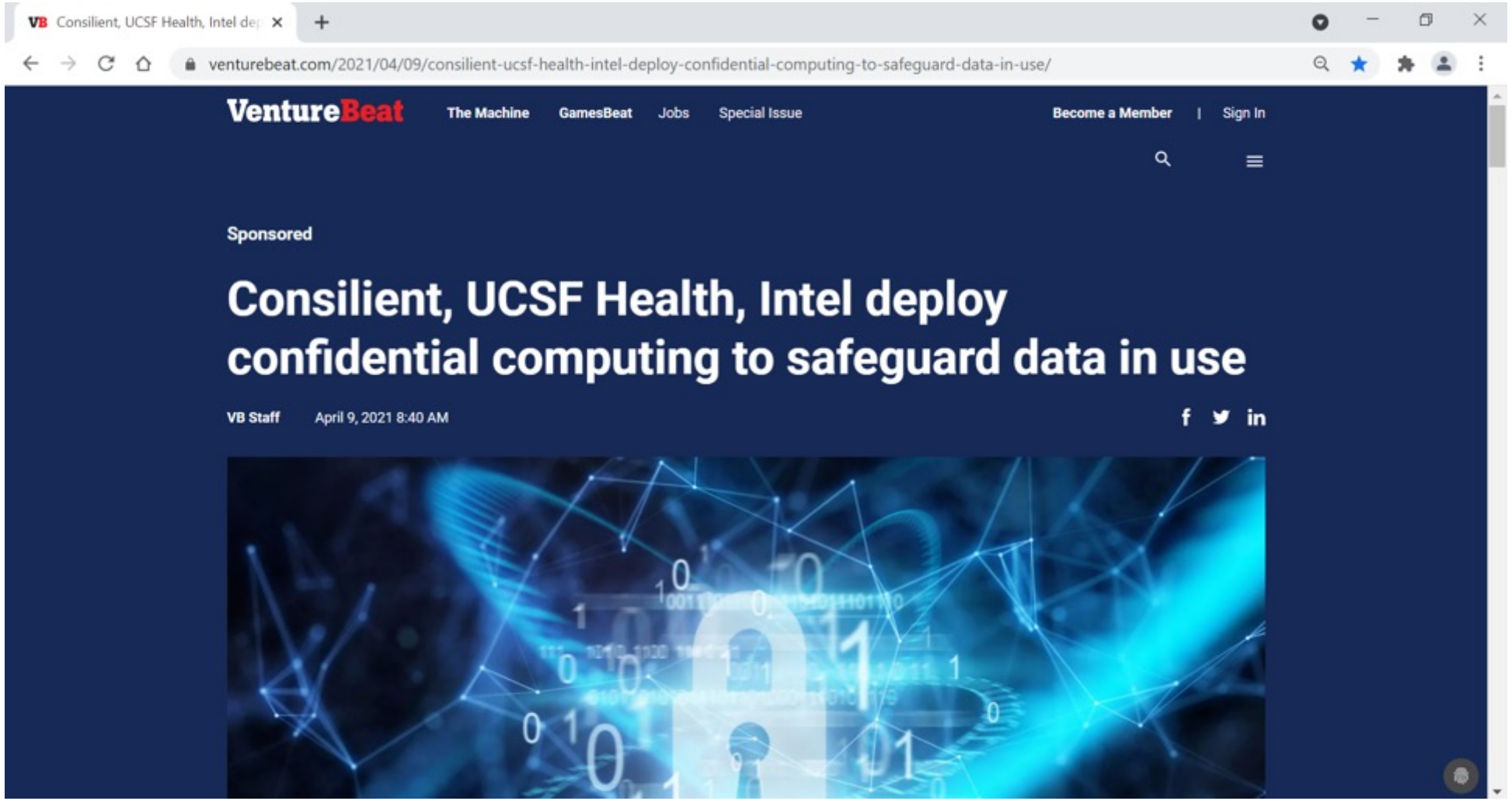
Co-founder & CTO

Fortanix

Vision and Perspective

- Problem
  - Confidential Computing – and other privacy-enhancing technologies (PETs) – need to integrate seamlessly with existing data and application workflows and scale according to requirements.
- Vision
  - Confidential Computing will be ubiquitous within cloud and on-premises compute resources.
  - Users can easily migrate workloads and develop applications across all available resources.
- Benefits
  - Data and application security can now be achieved at scale through close integration of Confidential Computing services with cloud architecture and data services.
  - Costs of deployment will diminish as Confidential Computing becomes a default method of deployment in the cloud and an integrated capability of OEM hardware.
  - End-to-end data security and applications control throughout the data lifecycle.

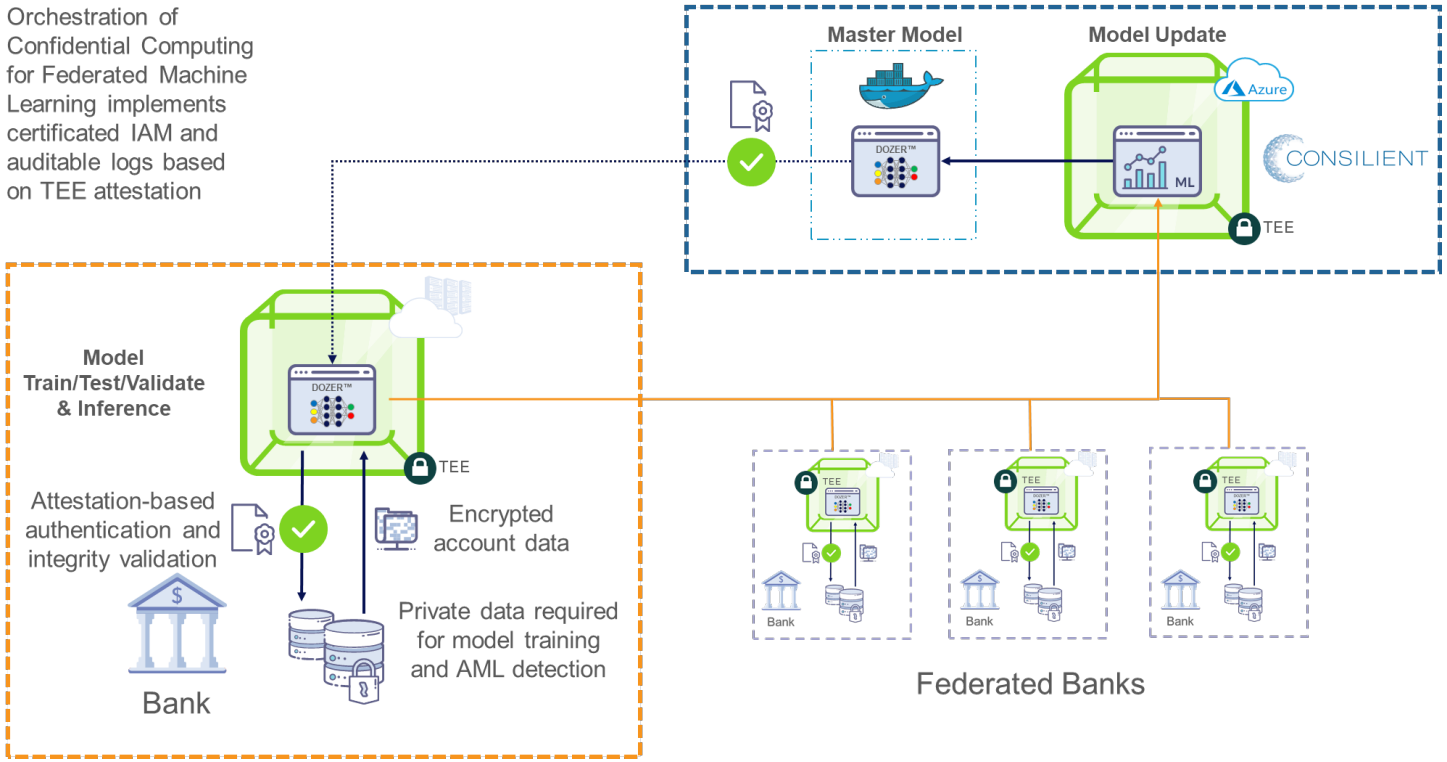
Confidential Computing in Practice



https://venturebeat.com/2021/04/09/consilient-ucsf-health-intel-deploy-confidential-computing-to-safeguard-data-in-use/

Use-Case: Consilient – Anti-Money Laundering

- Between **$800 million and $2 trillion** in illicit transactions flow through the global economy each year with **<1%** intercepted by law enforcement agencies.
- AI technology can enhance detection but requires massive amounts of heterogeneous bank data for training and testing.
- Federated Machine Learning (FML) enables distributed AI training but carries data privacy risks.
- Confidential Computing enables AI training and inference while protecting bank data in use and maintaining the integrity of the detection algorithm and the active model.

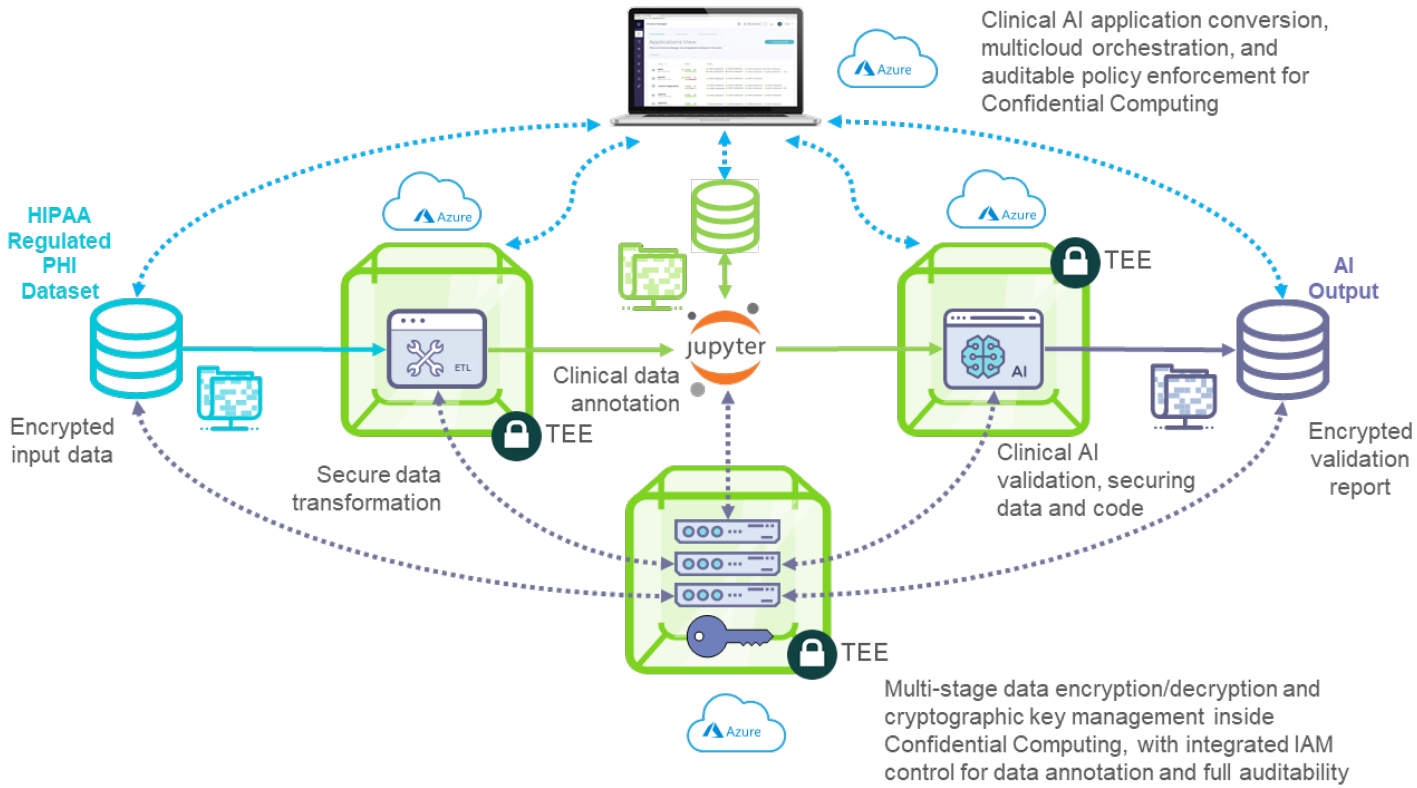


Use-Case: UCSF BeeKeeperAI™ – Clinical AI Validation

- Clinical AI validation requires access to PHI data via a protracted and costly approval process. Research often stalls.
- Confidential Computing enables protection of PHI data **and** protection of intellectual property within the algorithm code.
- With cloud scalability and auditable compliance, BeeKeeperAI™ enables rapid validation of AI to achieve US FDA approval.
- Estimated **55% - 75%** reduction in time to regulatory approval.
- Estimated cost saving of **~$2.0M** per algorithm, delivering healthcare and economic benefit to patients.

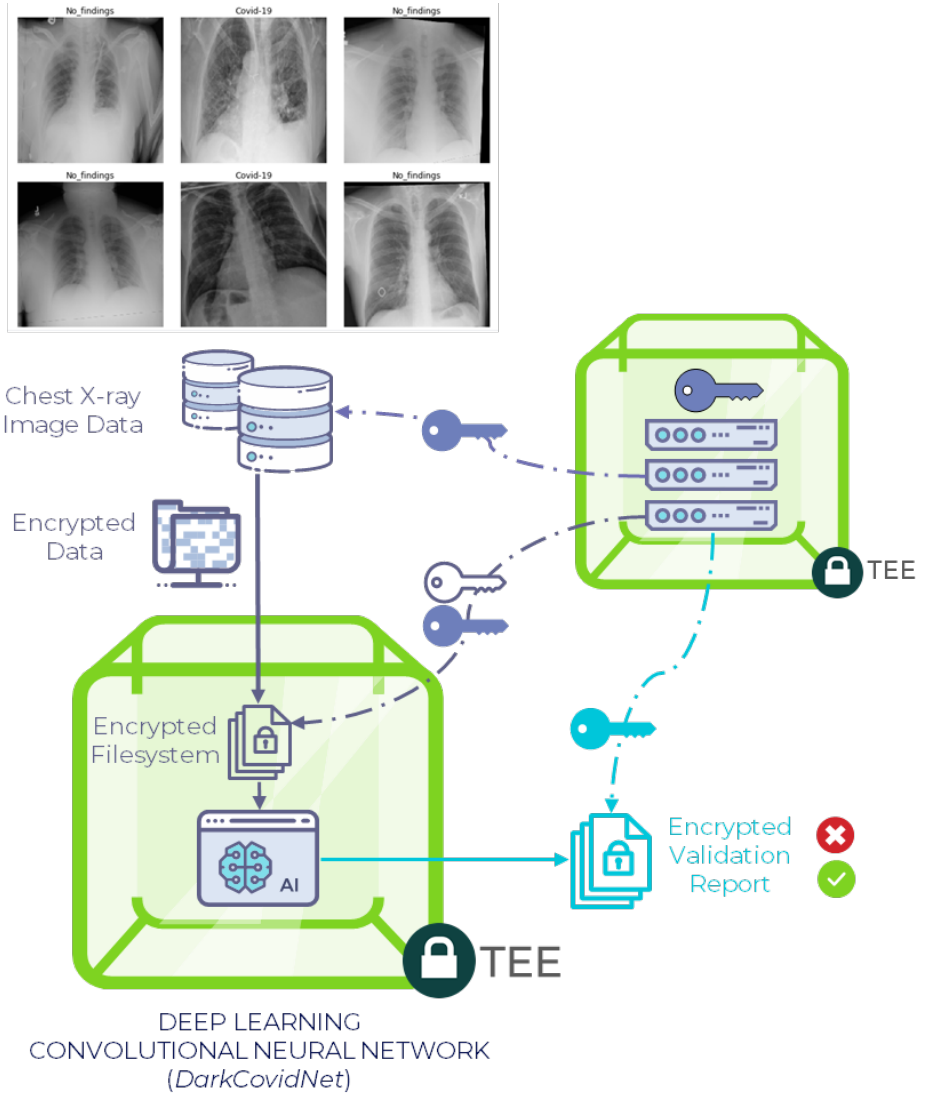
cdhi | Center for Digital Health Innovation at UCSF

BeeKeeperAI™



Use-Case Demonstration: AI Image Classification

- Confidential Computing offers rapid, scalable deployment of sensitive data and applications to provide end-to-end data security.
- The COVID-19 pandemic saw huge interest in Confidential Computing as an enabling technology for healthcare AI.
- In December 2020, *DarkCovidNet* demonstrated the convolutional neural network (CNN) protected by a TEE with equivalent functionality and comparable performance to unprotected implementations.
  - https://fortanix.com/blog/2020/12/securing-healthcare-ai-with-confidential-computing/



Demonstration

Buyers Guide/Critical Criteria

Things to look in your Confidential Computing solution:

- ✓Broad custom and off the shelf application support
- ✓Consistent/Easy to deploy on prem and in the cloud
  - ✓Cloud/hardware technology/version agnostic
  - ✓Lift and shift of apps/workloads/data
  - ✓Integrates with existing IT processes and systems
    - ✓Key management
    - ✓Containers/Kubernetes
    - ✓Management and monitoring
- ✓Ready and abstracted for the future
  - ✓New clouds/platforms
  - ✓Homomorphic encryption technologies

Learn More! Watch the Other Sessions in this Series

What is Confidential Computing and Why Should I Care?

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

Confidential Computing Protecting Data in Use

Watch on-demand: https://youtu.be/7XKTmL9bHV8

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!