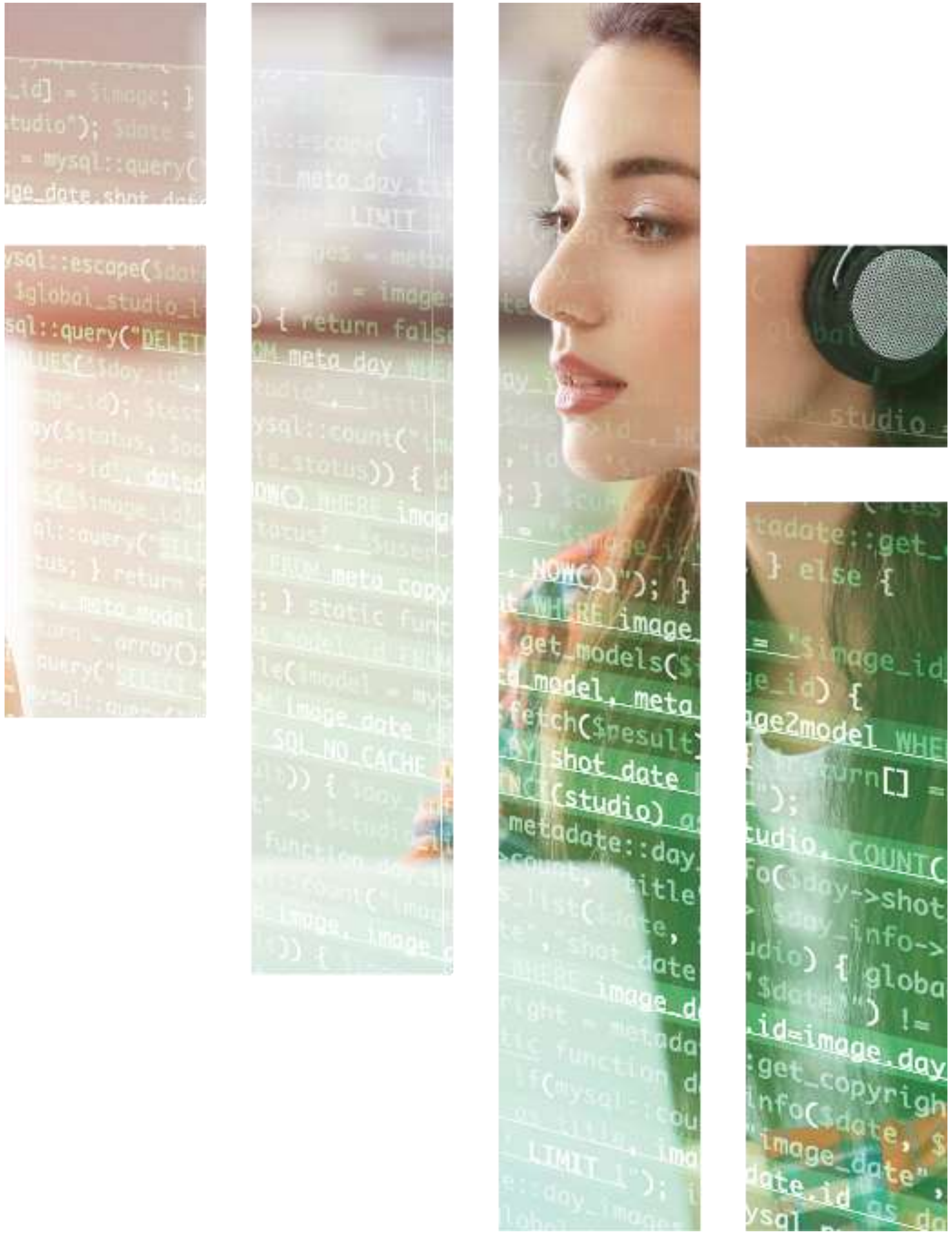
Demystifying Confidential Computing

A Game-Changer in the World of Privacy & Security

Dr Richard Searle

Vice President of Confidential Computing

Fortanix®



Fortanix

Founded in 2016
Ambuj Kumar, CEO & Co-founder
Anand Kashyap, CTO & Co-founder

MORE THAN 20 INDUSTRY AWARDS
RSA Innovation Sandbox Finalist
Gartner Cool Vendor

RSAC Innovation Sandbox 2018 RUNNER-UP
Gartner Cool Vendor 2018
Fortanix
Fortanix is proud to be recognized by cyber security industry
CYBER SECURITY EXCELLENCE AWARDS WINNER 2021
INFOSEC PRODUCTS OF THE MONTH
TMCnet .com Cybersecurity Excellence 2021
BIG INNOVATION 20 22
cyber secured AWARDS 2021

Fortanix® is the data-first security company and pioneer of Confidential Computing

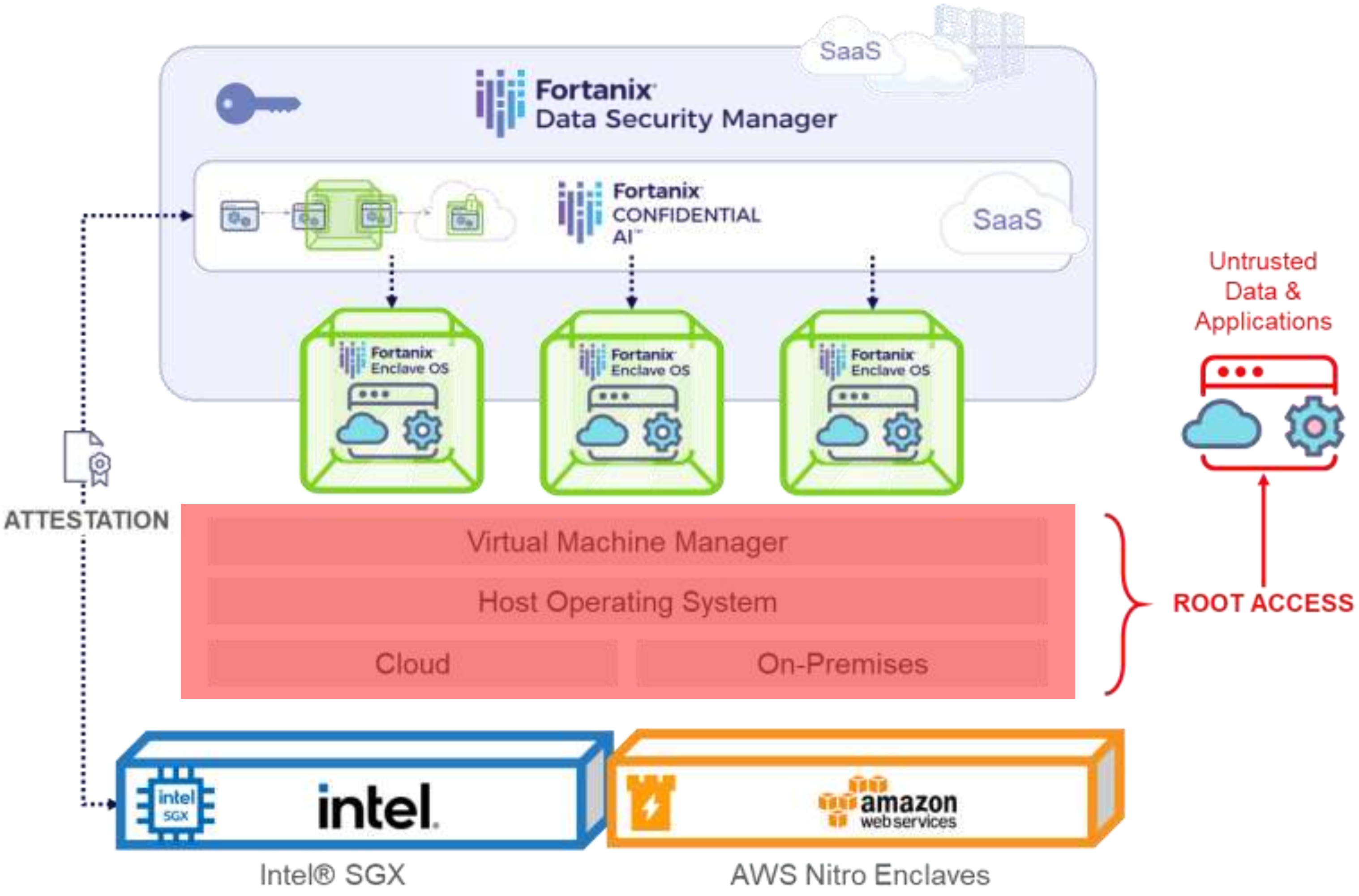
CONFIDENTIAL COMPUTING CONSORTIUM

Recently ranked as one of America's fastest growing companies

What is Confidential Computing?

Protecting Data In Use

CONFIDENTIAL COMPUTING CONSORTIUM
GENERAL MEMBER



SaaS

Fortanix Data Security Manager

Fortanix CONFIDENTIAL AI™

SaaS

Fortanix Enclave OS

Fortanix Enclave OS

Fortanix Enclave OS

ATTESTATION

Virtual Machine Manager

Host Operating System

Cloud

On-Premises

Untrusted Data & Applications

ROOT ACCESS

intel SGX

intel.

amazon web services

Intel® SGX

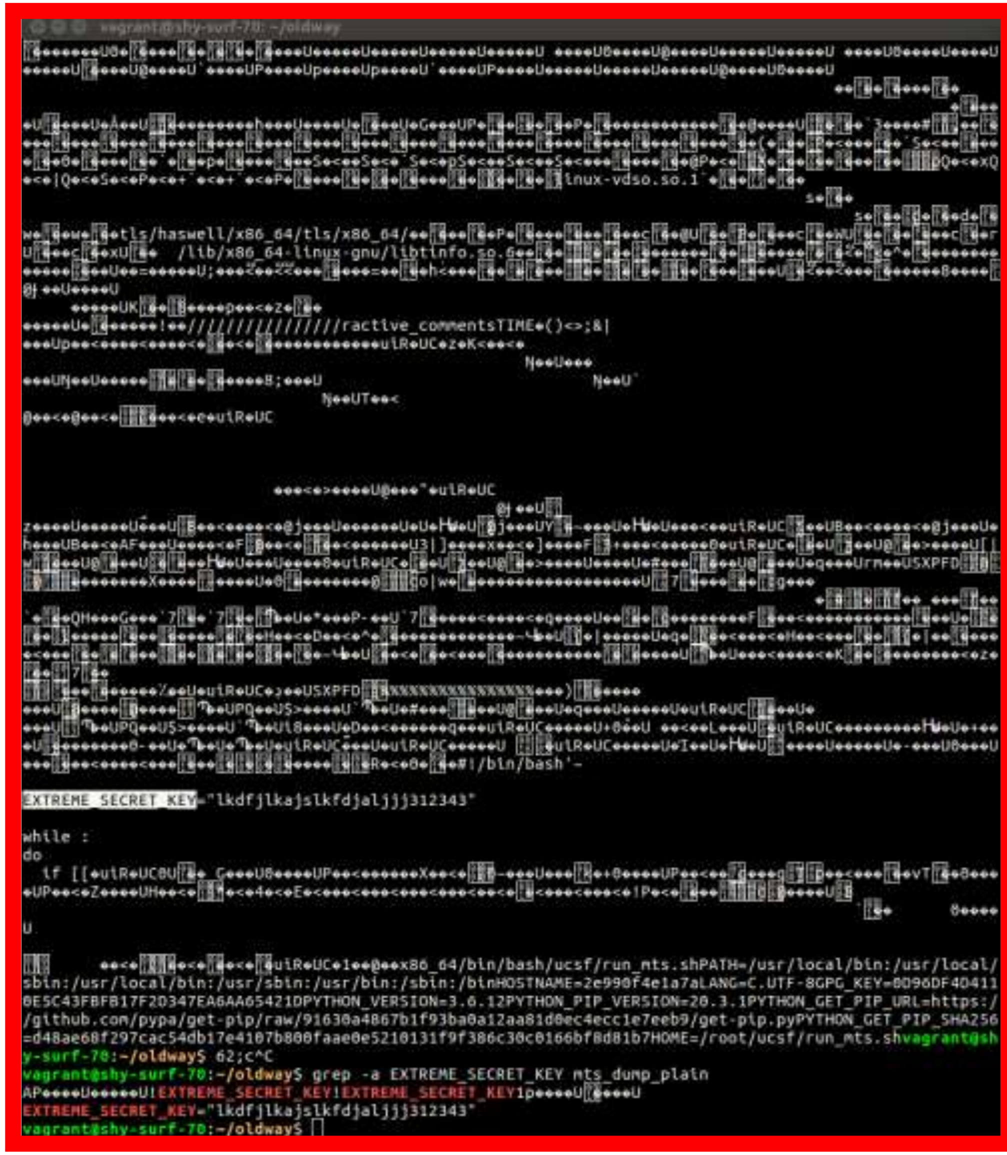
AWS Nitro Enclaves

> **"Confidential Computing is the protection of data in use by performing computation in a hardware-based attested Trusted Execution Environment."**
>
> \- Confidential Computing Consortium

Confidential Computing Deep Dive v1.0

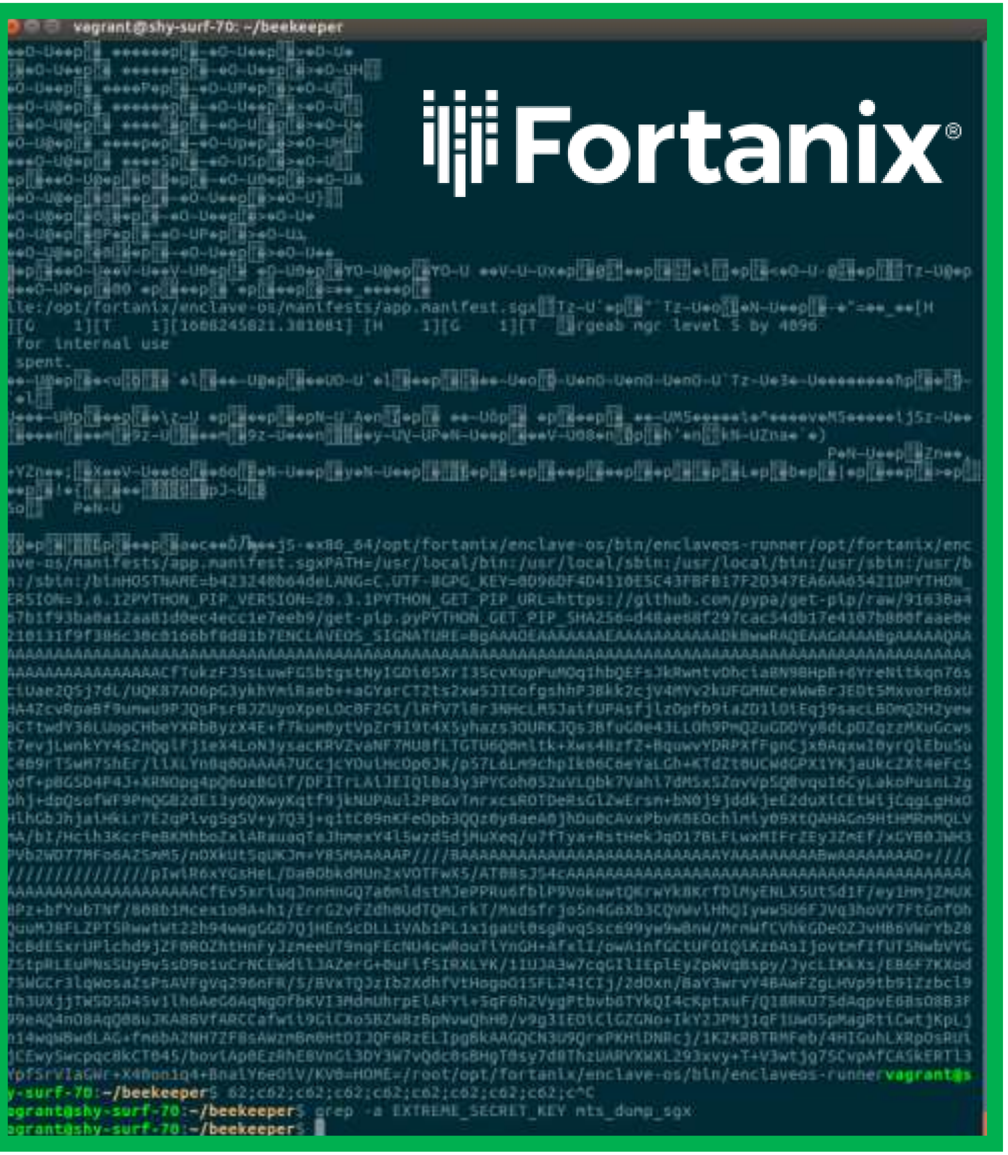
https://confidentialcomputing.io/white-papers/

Confidential Computing in Action



```
vagrant@shy-surf-70: ~/oldway
```

```
/lib/x86_64-linux-gnu/libtinfo.so.6
ractive_commentsTIME()<>;&|
#!/bin/bash'-

EXTREME_SECRET_KEY="lkdfjlkajslkfdjaljjj312343"

while :
do
  if [[

U

x86_64/bin/bash/ucsf/run_mts.shPATH=/usr/local/bin:/usr/local/
sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binHOSTNAME=2e990f4e1a7aLANG=C.UTF-8GPG_KEY=0D96DF4D411
0E5C43FBFB17F2D347EA6AA65421DPYTHON_VERSION=3.6.12PYTHON_PIP_VERSION=20.3.1PYTHON_GET_PIP_URL=https:/
/github.com/pypa/get-pip/raw/91630a4867b1f93ba0a12aa81d0ec4ecc1e7eeb9/get-pip.pyPYTHON_GET_PIP_SHA256
=d48ae68f297cac54db17e4107b800faae0e5210131f9f386c30c0166bf8d81b7HOME=/root/ucsf/run_mts.shvagrant@sh
y-surf-70:~/oldway$ 62;c^C
vagrant@shy-surf-70:~/oldway$ grep -a EXTREME_SECRET_KEY mts_dump_plain
APU!EXTREME_SECRET_KEY!EXTREME_SECRET_KEY1pU
EXTREME_SECRET_KEY="lkdfjlkajslkfdjaljjj312343"
vagrant@shy-surf-70:~/oldway$
```



```
vagrant@shy-surf-70: ~/beekeeper
```

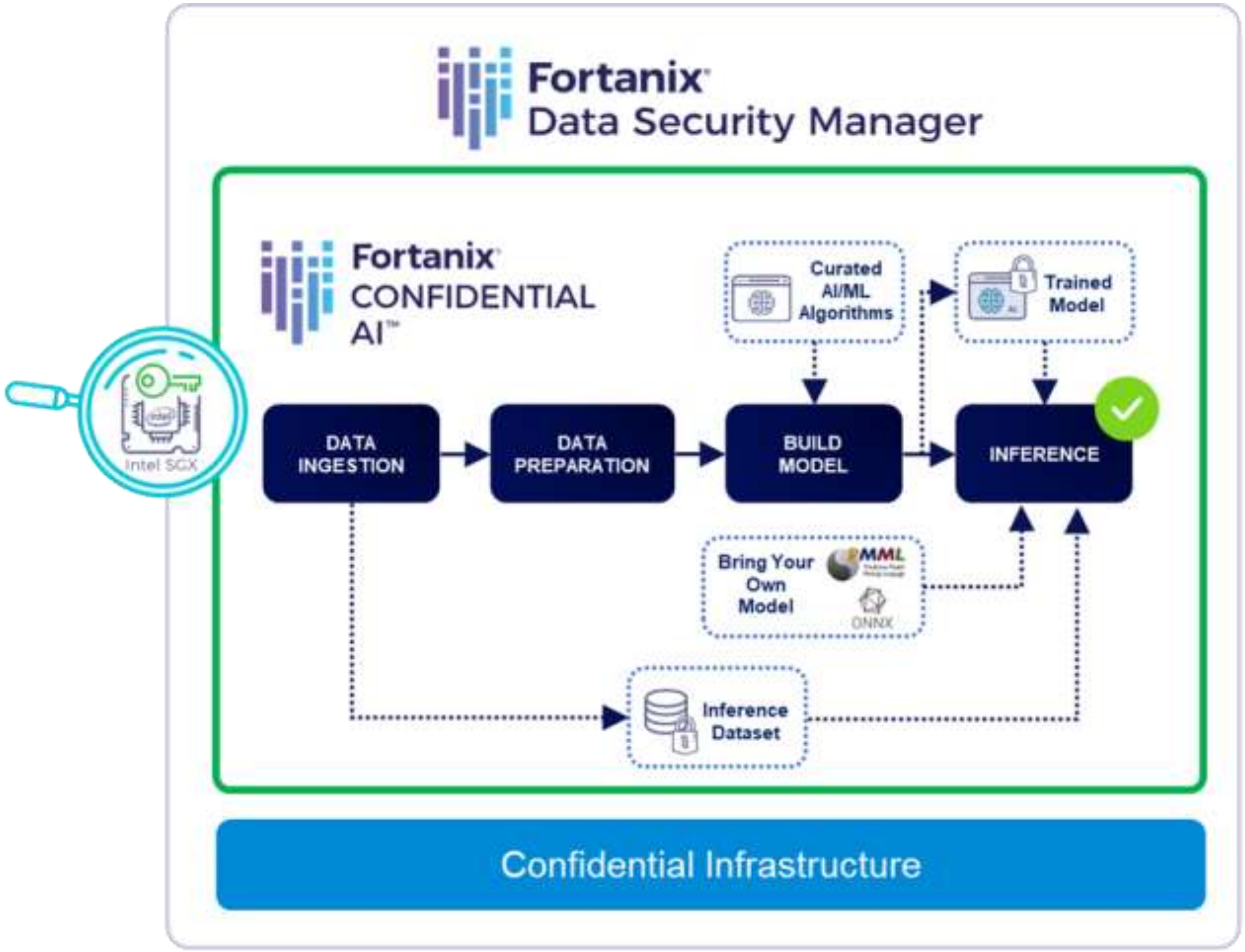
```
le:/opt/fortanix/enclave-os/manifests/app.manifest.sgx
 for internal use
 spent

x86_64/opt/fortanix/enclave-os/bin/enclaveos-runner/opt/fortanix/enc
ave-os/manifests/app.manifest.sgxPATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/b
n:/sbin:/binHOSTNAME=b42324Bb64deLANG=C.UTF-8GPG_KEY=0D96DF4D4110E5C43FBFB17F2D347EA6AA65421DPYTHON_
ERSION=3.6.12PYTHON_PIP_VERSION=20.3.1PYTHON_GET_PIP_URL=https://github.com/pypa/get-pip/raw/91630a4
67b1f93ba0a12aa81d0ec4ecc1e7eeb9/get-pip.pyPYTHON_GET_PIP_SHA256=d48ae68f297cac54db17e4107b800faae0e
210131f9f386c30c0166bf8d81b7ENCLAVEOS_SIGNATURE=BgAAADEAAAAAAAEAAAAAAAAAAADkBwwRAQEAAGAAAABgAAAAQAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAACfTukzFJ5sLuwFGSbtgstNyIGDi65XrI35cvKupFuMOq1hbQEFsJkRwmtvDbciaBN98HpB+6YreNitkqn76s
HOME=/root/opt/fortanix/enclave-os/bin/enclaveos-runnervagrant@s
y-surf-70:~/beekeeper$ 62;c62;c62;c62;c62;c62;c62;c62;c62;c^C
agrant@shy-surf-70:~/beekeeper$ grep -a EXTREME_SECRET_KEY mts_dump_sgx
agrant@shy-surf-70:~/beekeeper$
```

Fortanix®

How is Confidential Computing Transforming Privacy and Security for Data and Applications?

- Confidential Computing closes the loop by protecting **data in use** – **full-lifecycle data security**
- Confidential Computing supports **deployment flexibility and workload explainability**
- Compatible infrastructure is now available from **all major cloud service providers**
- Attestation supports **zero-trust** application **authentication and integrity verification**
- Confidential Computing proving a **disruptive source of business innovation**

Confidential Computing Made Simple with Fortanix

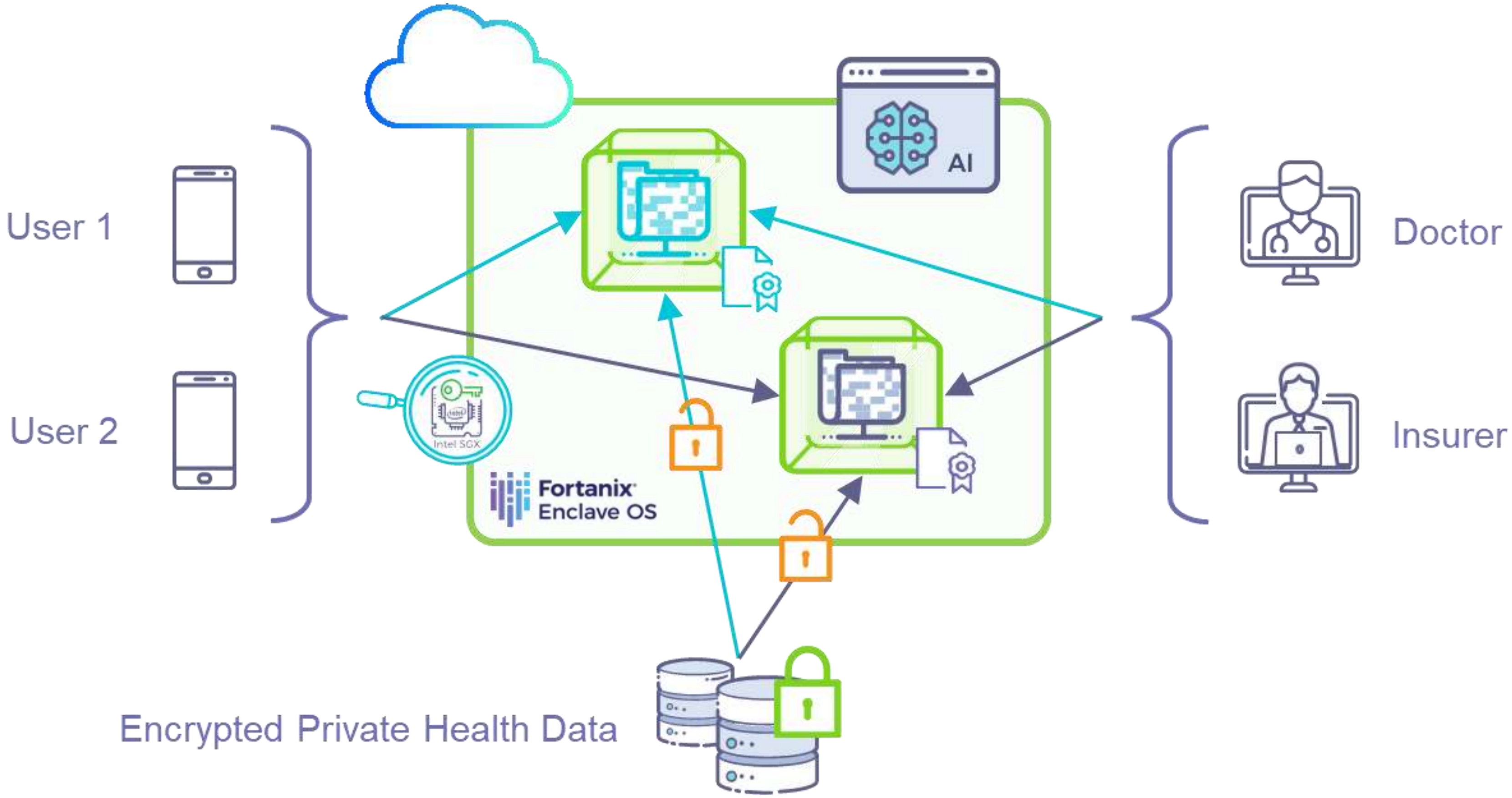


PyTorch TensorFlow scikit learn PMML Predictive Model Markup Language ONNX

Examples of Confidential Computing Today

Enabling User Control of PHI

- Protecting electronic health records (eHR) for up to 75M German citizens
- Enabling patient control over protected healthcare information (PHI) under EU GDPR
- Scalable from the initial production service launch on 1 January 2021

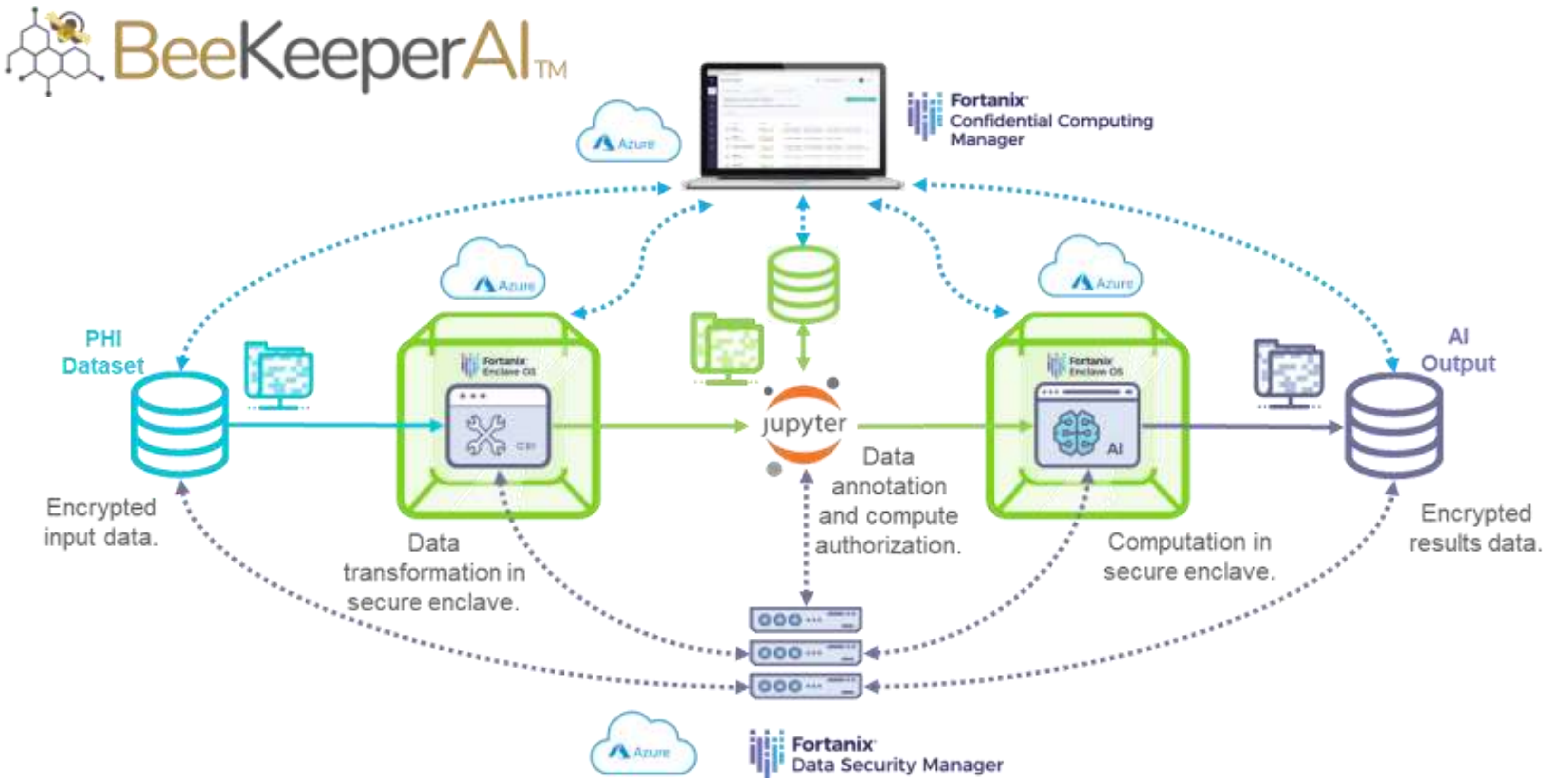


Accelerating Healthcare AI

BeeKeeperAI is a pioneer in combining zero trust, confidential computing, and privacy preserving analytics for the training, validation, and deployment of artificial intelligence.

"As the former Chair of the IT Security committee at UCSF, I developed a deep appreciation for the need to secure our data while making it available to advance the mission of the organization."

Michael Blum, MD
Co-founder & CEO of BeeKeeperAI


BeeKeeperAI™
Azure
Fortanix Confidential Computing Manager
PHI Dataset
Encrypted input data.
Azure
Fortanix Enclave OS
Data transformation in secure enclave.
jupyter
Data annotation and compute authorization.
Azure
Fortanix Enclave OS
AI
Computation in secure enclave.
AI Output
Encrypted results data.
Azure
Fortanix Data Security Manager

Today

- 16-30 months an $1.5-$2M to validate an algorithm
- Secure compute on protected data – unable to leverage cloud
- Protracted contractual negotiations to ensure privacy

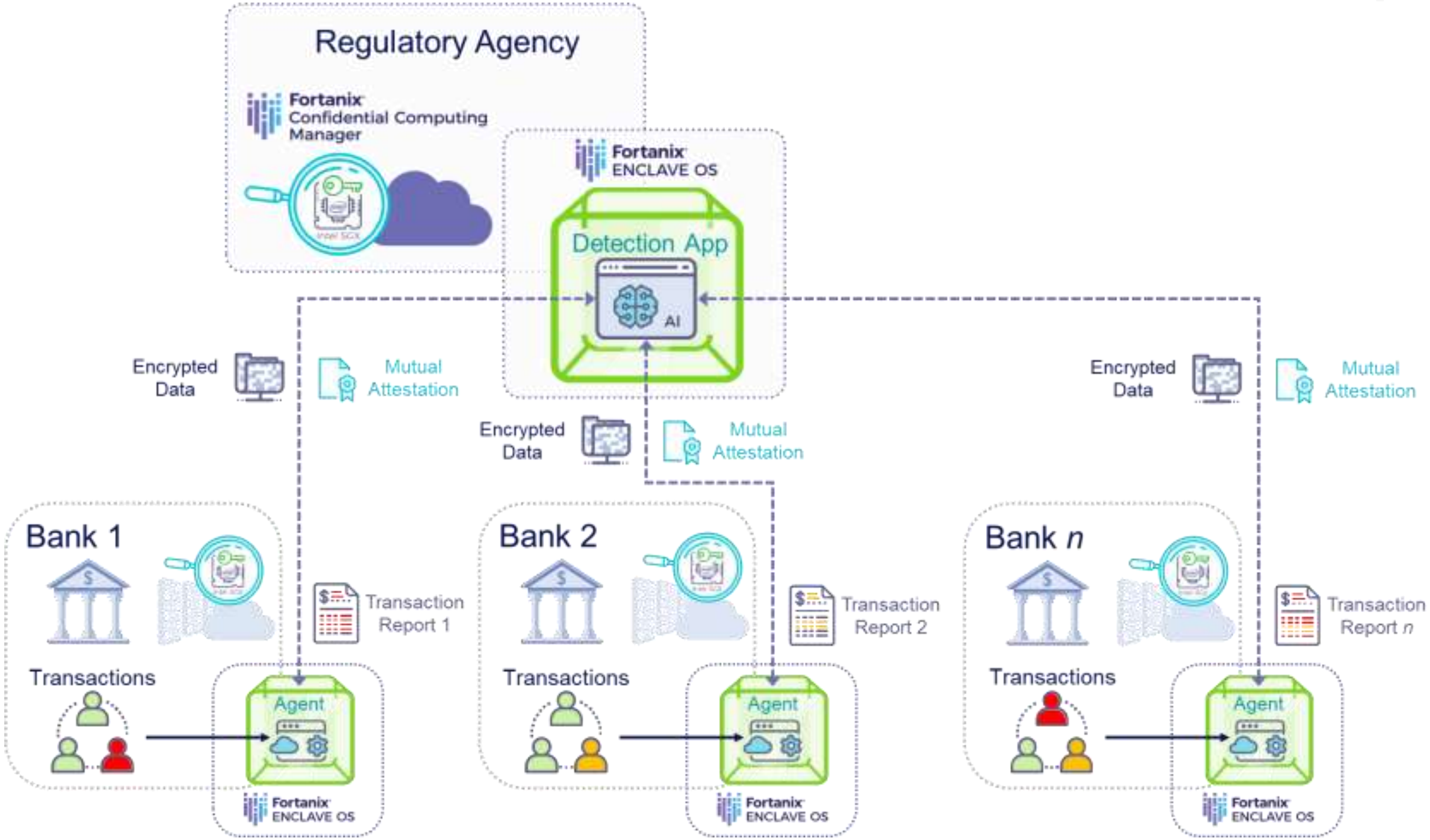
With Confidential Computing

- 1000x acceleration in time to market
- End-to-end encryption of all private data with zero trust
- Streamlined workflow for regulatory approval of healthcare AI systems

Preventing Financial Crime

- Sythentic-identity fraud detection with FiVerity
- Banks are able to share encrypted account data and network telemetry for aggregated data analysis
- Banks can demonstrate PII data compliance using attestation logs
- Multi-jurisdiction support

FIVERITY

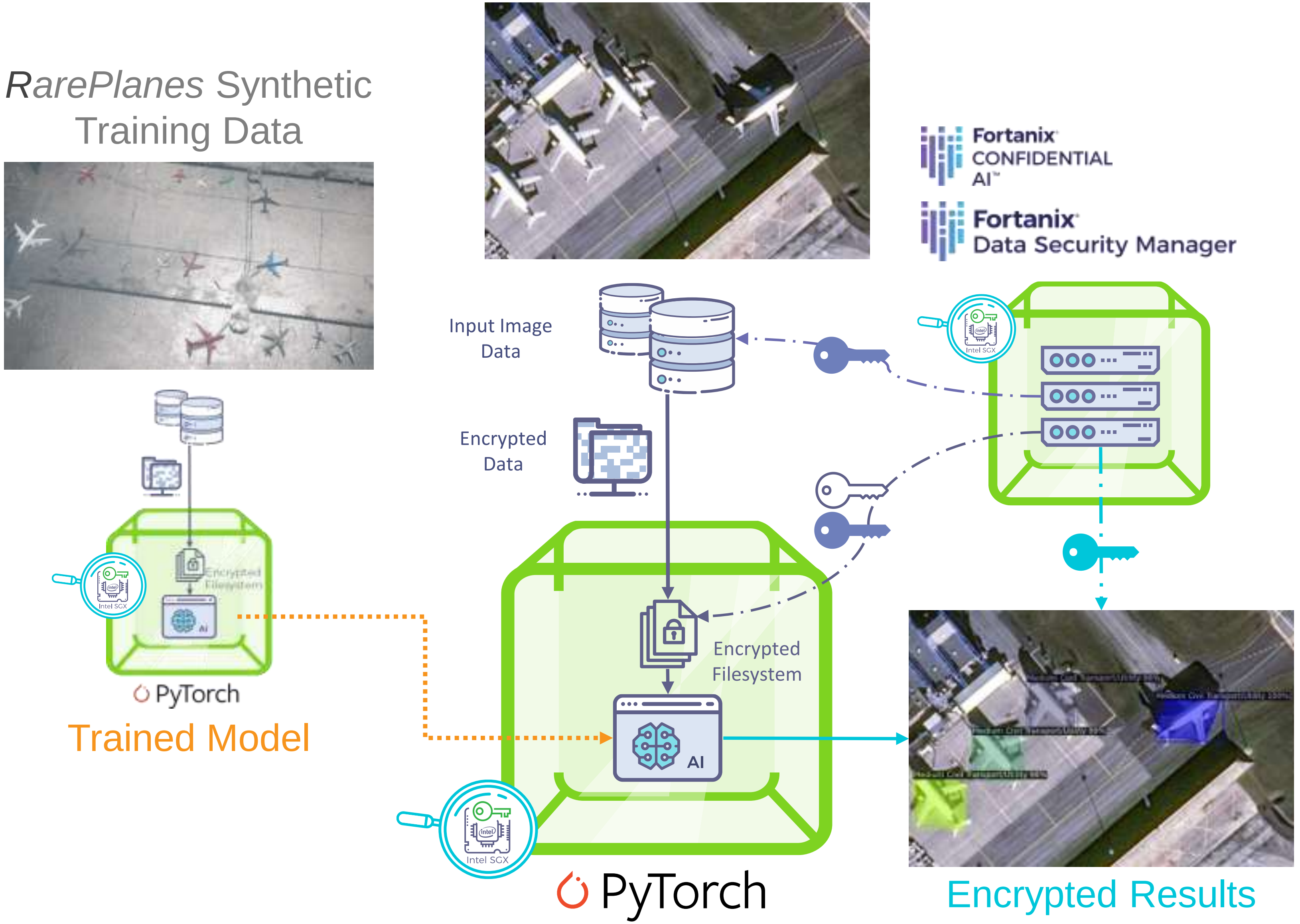


Securing Sensitive Data

- Object detection and classification
- Protecting sensitive information and confidential algorithms
- Deployable with all major AI/ML frameworks
- Protects against adversarial machine learning attacks

RarePlanes Synthetic Training Data

Real Satellite Data



Satellite images: © CNES 2016, Distribution Airbus DS.

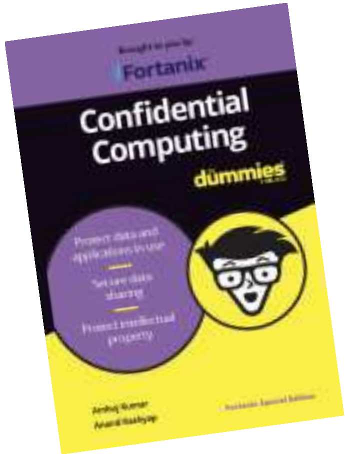
Thank You

Aqaio

Stand 7-243

Visit us to find out more!

- fortanix.com
- info@fortanix.com
- @fortanix
- Fortanix



https://resources.fortanix.com/confidential-computing-for-dummies-fortanix-special-edition

Fortanix®