BeeKeeperAI™

Enabling ethical & secure computing on PHI data

Fall 2022

Permission for use

This presentation may be shared within Microsoft as well with Microsoft partners and customers in which an NDA is currently in effect.

Healthcare AI is not reaching the bedside!

93%[1]	6%	0%	1%	0%
AI Research & Development	Proof of AI Value	Deployment Testing	Commercial Deployment	Monitoring & Optimization

BeeKeeperAI™

De-identified Data	Computing on Protected Health Information (PHI)
Data is Shared or Laked	Data and all computation occurs within the data steward's HIPAA compliant cloud environment
Signal Finding, Inference, Training	Validation, valuation, deployment & monitoring (inference and training are also supported by BeeKeeperAI)

[1]The number of published biomedical AI studies within the phases of the AI development lifecycle

BeeKeeperAI™

A confidential computing, **zero-trust platform enabling** sightless computing where:

- PHI never leaves the data steward's HIPAA compliant environment
- PHI is never seen nor shared
- Algorithm intellectual property is protected

Optimal use cases for BeeKeeperAI

Using protected health information (PHI) safely, securely, and ethically

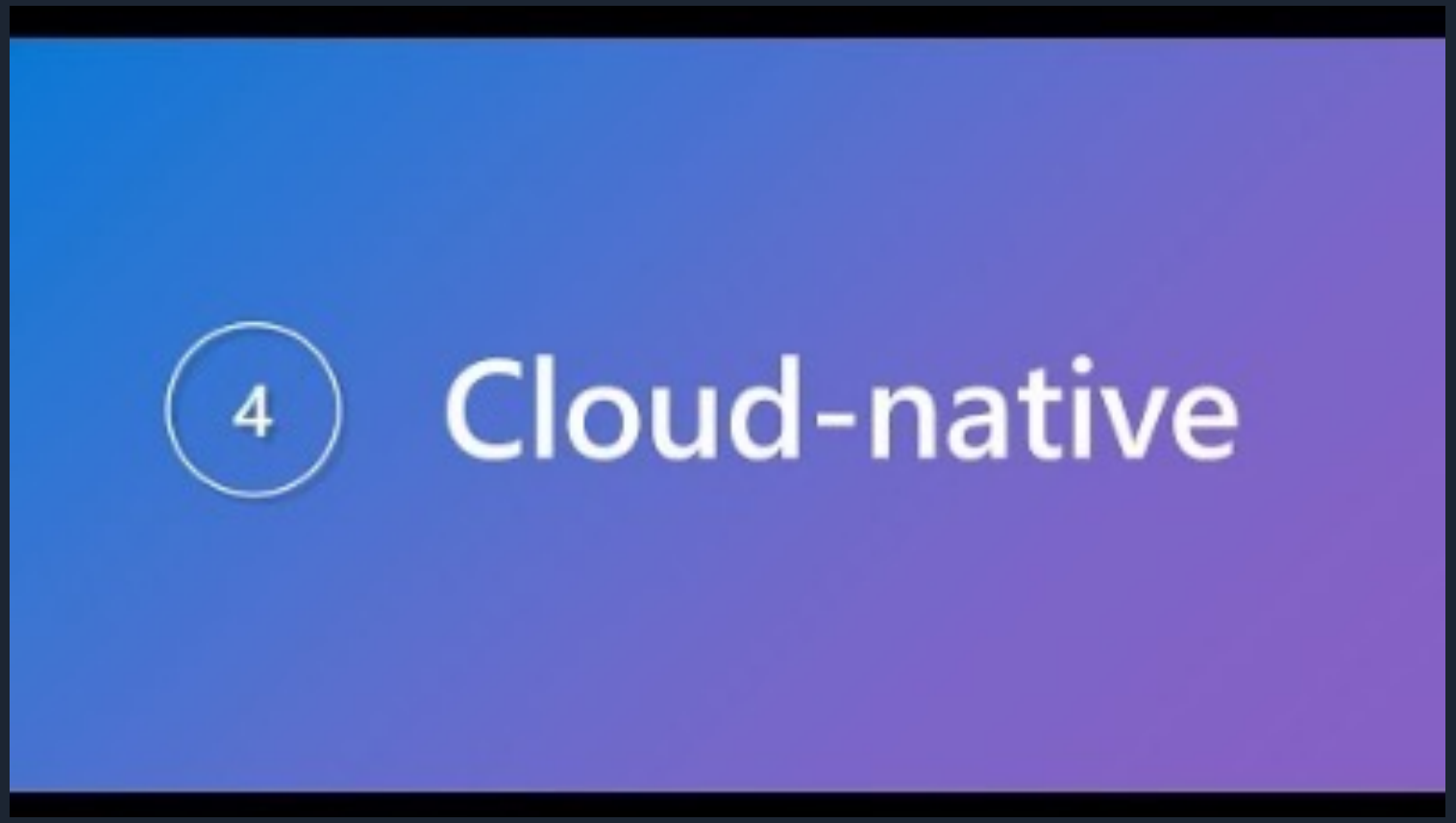
Optimal for any project requiring:

- Data that can not be de-identified (e.g., retinal images, genomic data, etc.)
- Data that is too sensitive to risk exposure (e.g., mental health, etc.)
- Small data sets that risk re-identification (e.g., rare disease)
- Data de-identification tools and effort would be cost prohibitive

"Without BeeKeeperAI we would not have the ability to test algorithms we believe can make a real impact for at risk patients and for the healthcare providers tasked with diagnosing and caring for them."

Robin Roberts, Co-Founder / COO & Head of Strategy Novartis Biome, Novartis Pharmaceuticals Corporation

SaaS application hosted in Microsoft Azure infrastructure

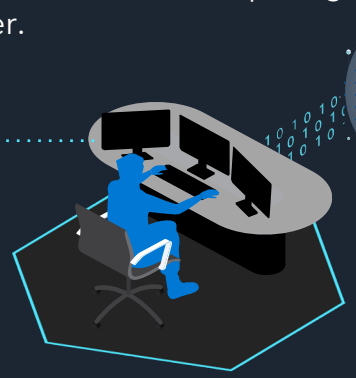


Satya Nadella
Microsoft CEO
Opening Keynote at BUILD 2022

Confidential, sightless computing infrastructure

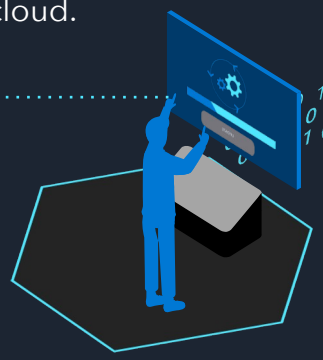
Algorithm Owner submits an encrypted algorithm where it is wrapped in a secure computing container.

1



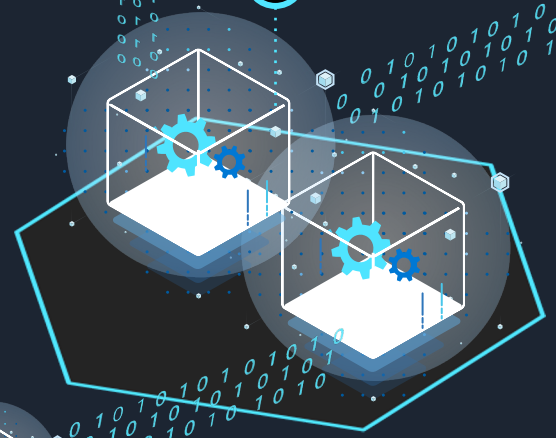
Data Steward(s) curates a data set to the algorithm requirements, encrypts it, and uploads it in a BeeKeeperAI accessible zone within their secure, HIPAA compliant cloud.

2



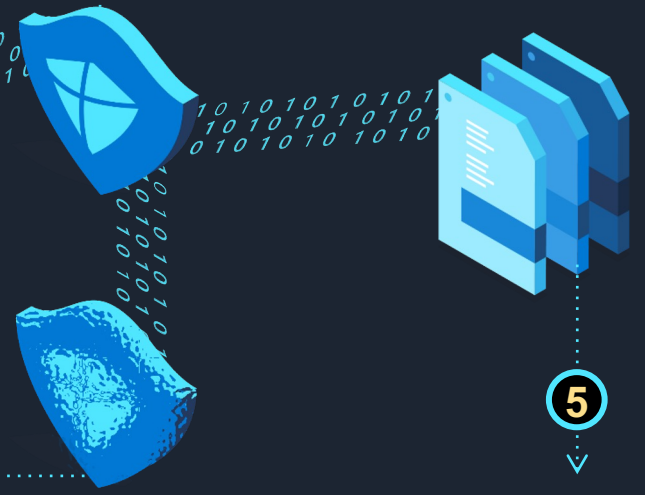
The secure container moves into the Data Steward's secure environment where is it merged with the encrypted data in an attested compute enclave.

3



4

The data set and algorithm are decrypted, the algorithm runs, and a confidential performance report is created.



5

The Algorithm Owner's performance report is the only thing that leaves the computing enclave.

6

If not required for additional runs or regulatory artifacts, the data set and algorithm within the enclave are destroyed and the enclave is decommissioned.

BeeKeeperAI™

Advantages: Easy to implement & highly secure

Microsoft | Azure Marketplace

Microsoft Azure

A healthcare friendly, HIPAA compliant, confidential computing environment required to store data, transport the model, and access the Intel hardware.

intel

Software Guard Extension (SGX) technology provides the processor-based vault where the algorithm runs against the encrypted data.

"In my opinion, BeeKeeperAI, with its end-to-end encryption and zero-trust environment, provides optimal security and the lowest cyberattack surface for both data and algorithms while enabling healthcare organizations to securely advance their innovation mission."

Marc d. Paradis, Vice President, Data Strategy, Northwell Holdings

Additional advantages

Let’s change the future together.