BeeKeeperAI®

Reducing the cost and time to market of healthcare AI
A zero-trust platform connecting data and algorithm owners

$42.5B healthcare AI market by 2026

The **promise** of healthcare AI:

AI has the potential to **improve outcomes by 30-40% while cutting treatment costs by as much as 50%**

The **problem** of healthcare AI:

Timely access to highly diverse, <u>real-world</u> data is the major barrier to achieving the promise of healthcare AI

~31 AI models have been approved by the FDA for use in healthcare (only 2 De Novo approved)

"Many researchers invest a significant amount of time in accessing the data and making it analyzable; this aspect needs to be improved." - Francis Collins, MD, PhD NIH Director

BeeKeeperAI™

BeeKeeperAI
changes the data access conversation

Applying privacy-preserving analytics to multi-institutional sources of protected data in a confidential computing environment in which . . .

- **Data never moves**
- **Data is never shared**
- **Algorithm IP is protected**

BeeKeeperAI™

BeeKeeperAI delivers value to stakeholders

Data Stewards

Maintain control of our data while accelerating our ability to fulfill our research mission

Enhance Competitiveness

Algorithm Owners

Protect our IP and gain timely access to the data required to achieve generalizability

12-mo Reduction of Time
$1-3M/model Savings

Researchers

Make novel discoveries by enabling the utilization of multi-site, rare data sets

12-mo Reduction of Time
Acceleration of Novel Discoveries
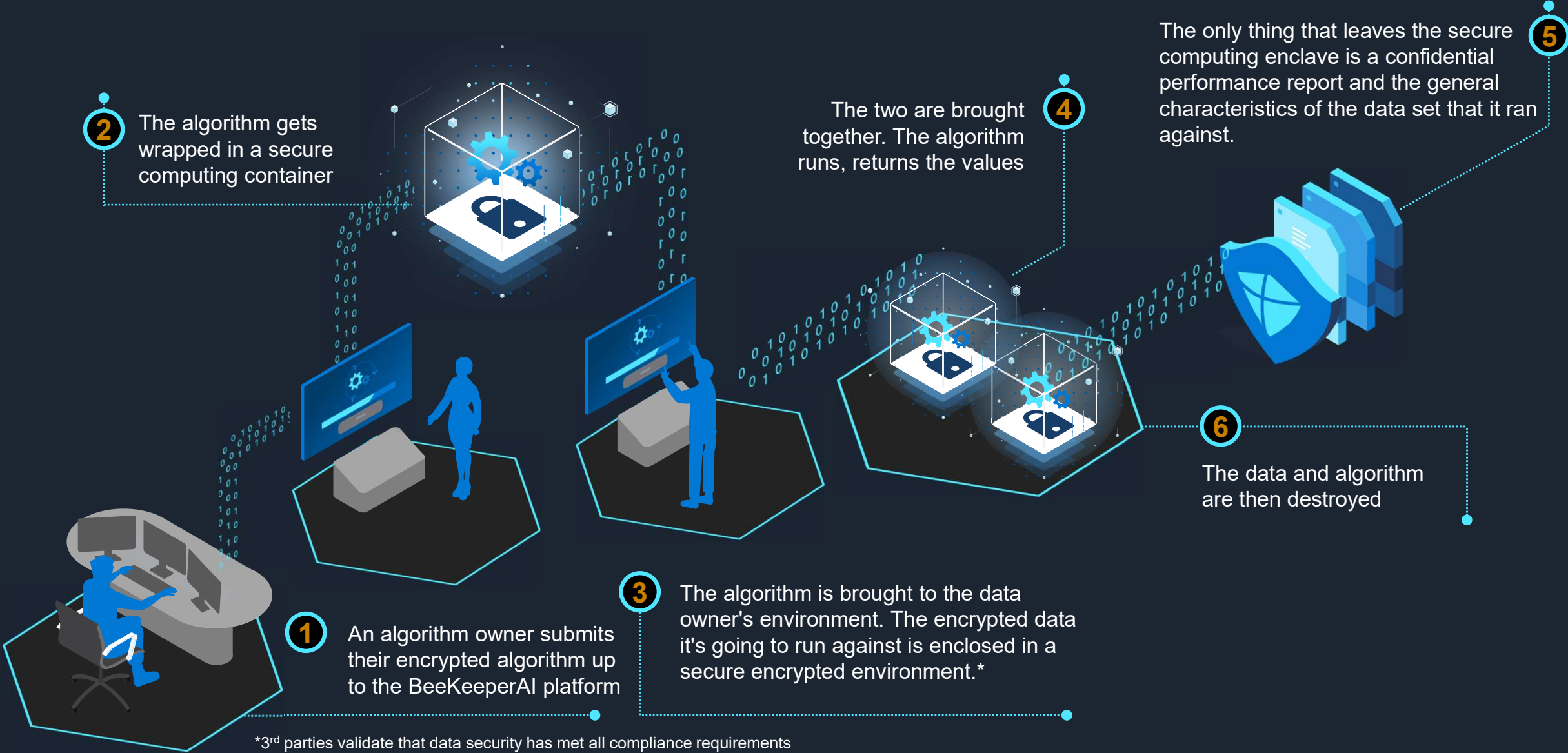
BeeKeeperAI™

Welcome to the future!

In June of 2021 third-party algorithm models
were sent via Azure Confidential Computing
to two data stewards' secure environments
where the models could not be seen
while they ran on data the algorithm developers could not see.

No one saw anything, not even BeeKeeperAI.

BeeKeeperAI™

How it works

2 The algorithm gets wrapped in a secure computing container

4 The two are brought together. The algorithm runs, returns the values

5 The only thing that leaves the secure computing enclave is a confidential performance report and the general characteristics of the data set that it ran against.

6 The data and algorithm are then destroyed

1 An algorithm owner submits their encrypted algorithm up to the BeeKeeperAI platform

3 The algorithm is brought to the data owner's environment. The encrypted data it's going to run against is enclosed in a secure encrypted environment.*

*3rd parties validate that data security has met all compliance requirements

BeeKeeperAI™
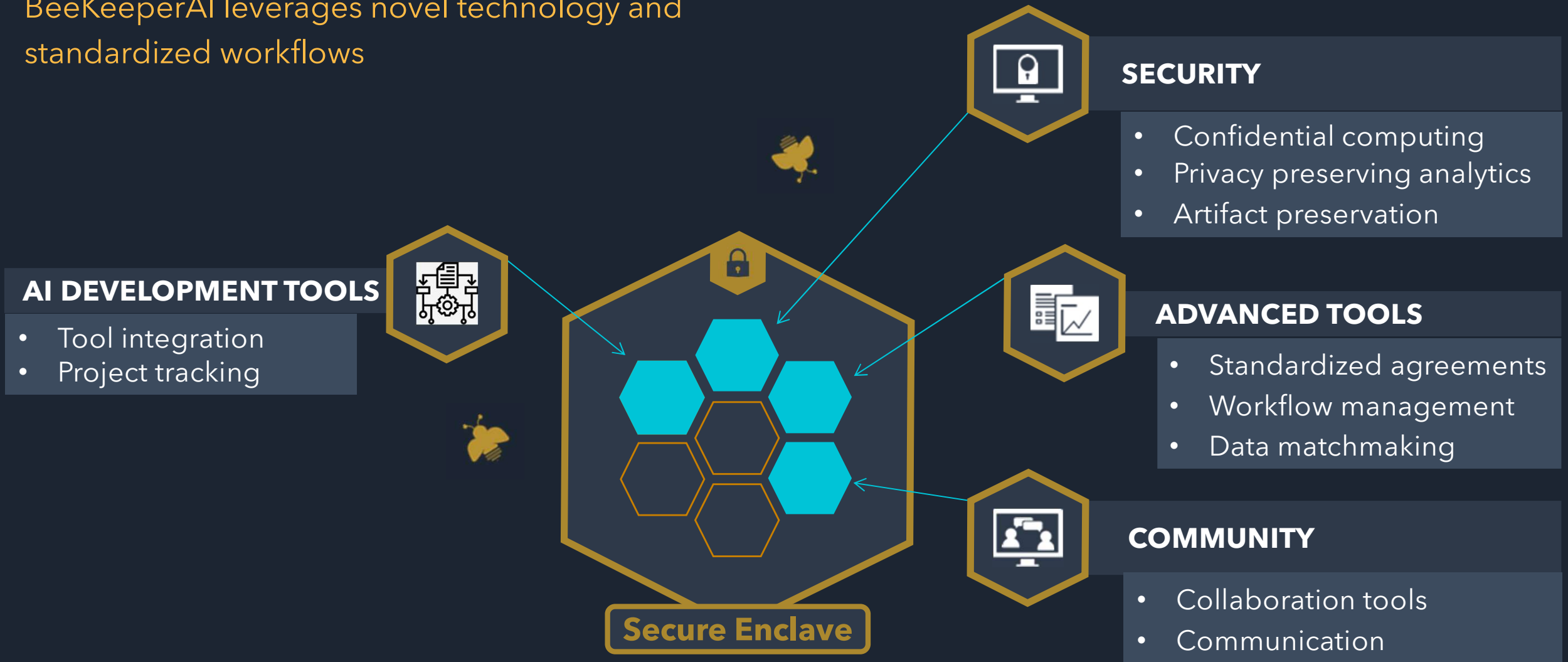
Our platform is designed to accelerate collaboration

BeeKeeperAI leverages novel technology and standardized workflows

SECURITY
- Confidential computing
- Privacy preserving analytics
- Artifact preservation

AI DEVELOPMENT TOOLS
- Tool integration
- Project tracking

ADVANCED TOOLS
- Standardized agreements
- Workflow management
- Data matchmaking

COMMUNITY
- Collaboration tools
- Communication

Secure Enclave

BeeKeeperAI™

Let's change the future together.