MITHRIL SECURITY

Confidential AI made easy

Privacy and security are blocking **AI adoption**

Analysis of medical documents

Hospitals fear sharing **documents with Cloud AI**

Targeted advertising

Third-party cookie removal pushes **privacy-friendly targeting**

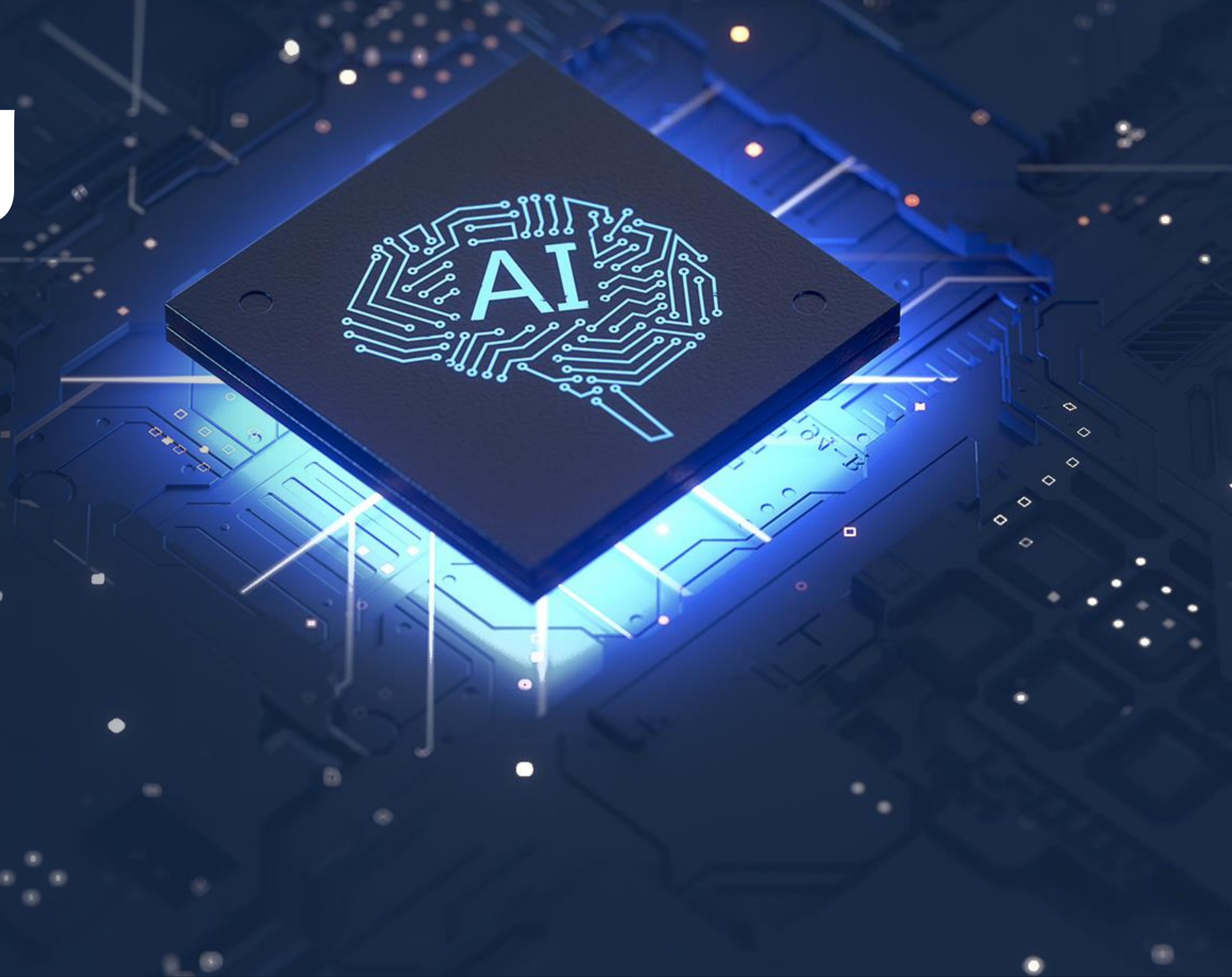
Biometric identification

Regulator **blocks AI identification in airports** because of privacy

MITHRIL SECURITY

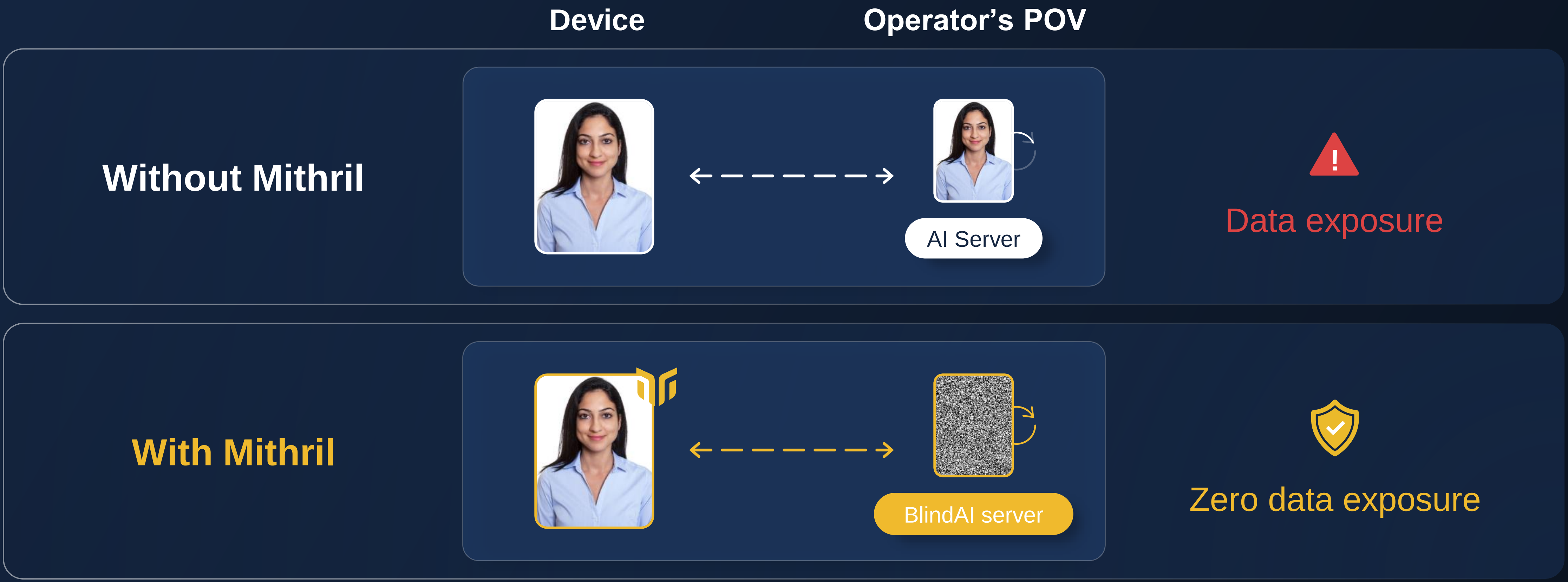
Introducing BlindAI

an Open-source and secure solution to analyze data confidentially



Example:
Biometric identification

Deploy compliant and privacy friendly biometric identification



Device

Operator’s POV

Without Mithril

AI Server

Data exposure

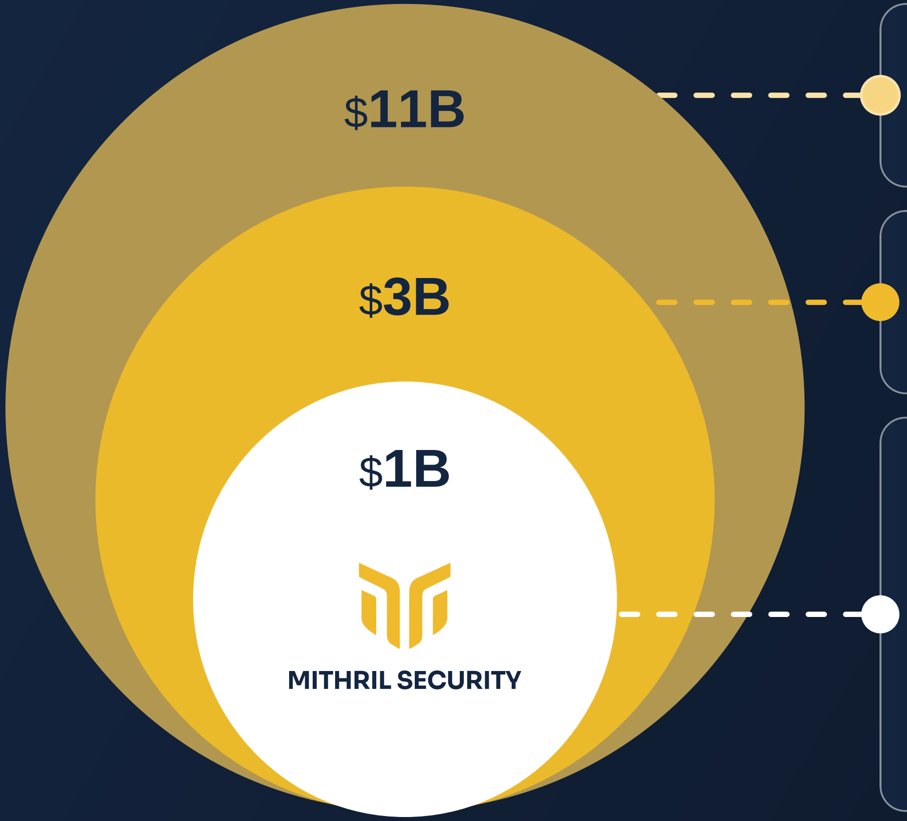
With Mithril

BlindAI server

Zero data exposure

MITHRIL SECURITY

Confidential Computing is hot with a 90% CAGR



Confidential Computing **software market**

Confidential Computing **AI software** market

Mithril **initial targets:**

› Biometrics

› Advertising

Early traction

Advertising

$80k
POC

Privacy_friendly **advertising**

Biometrics

$10k
POC

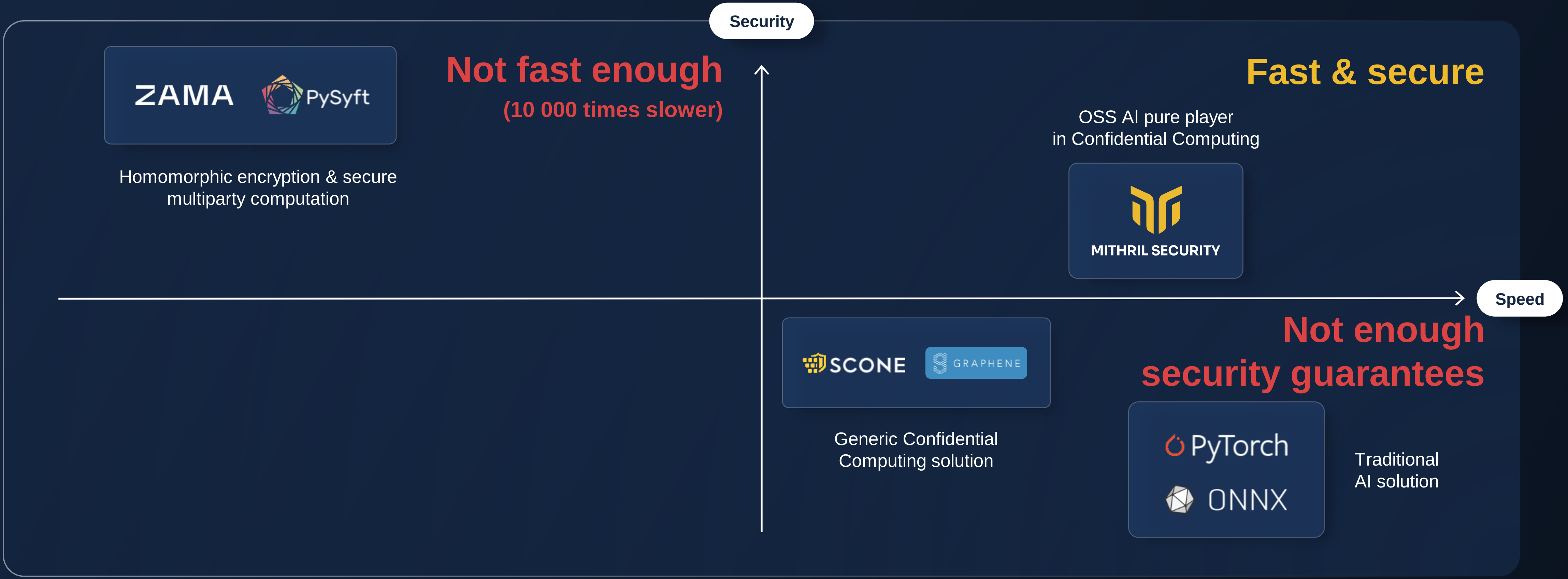
Biometric identification

Banking

Technical dive-in

KYC

We provide the best speed/security



Not fast enough
(10 000 times slower)

Homomorphic encryption & secure multiparty computation

Fast & secure

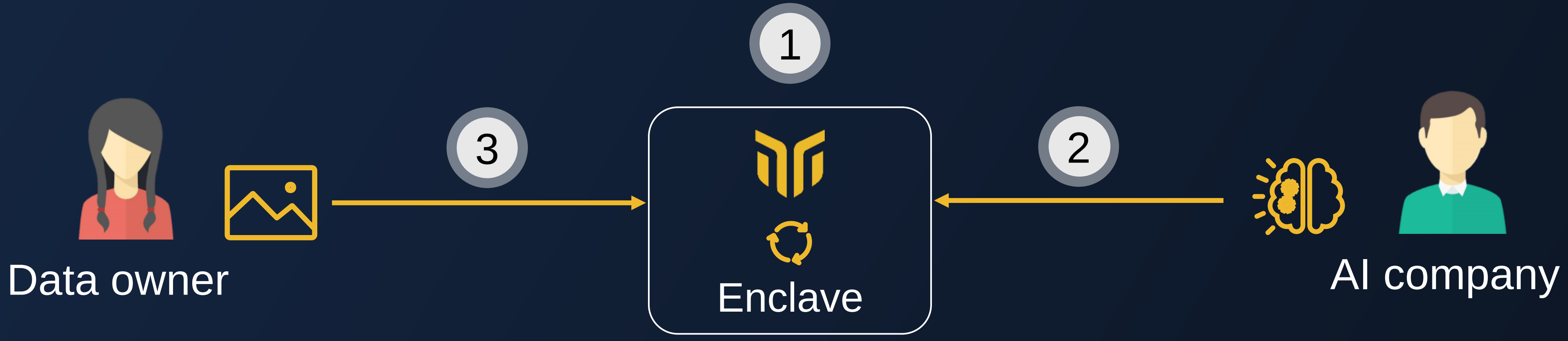
OSS AI pure player
in Confidential Computing

Generic Confidential Computing solution

Not enough security guarantees

Traditional
AI solution

Workflow with BlindAI



1

Launch server

with hardware protection

2

Upload model

In secure environment

3

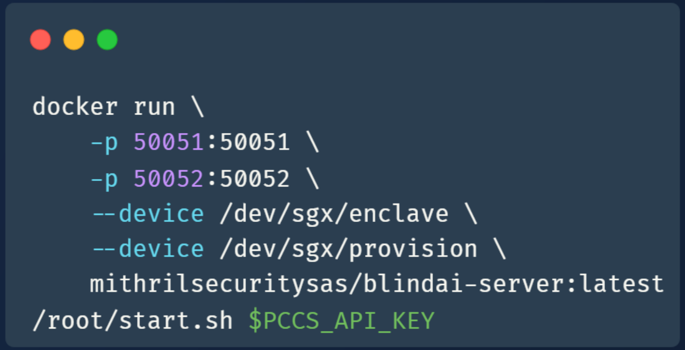
Get prediction

with confidentiality guarantees

MITHRIL SECURITY

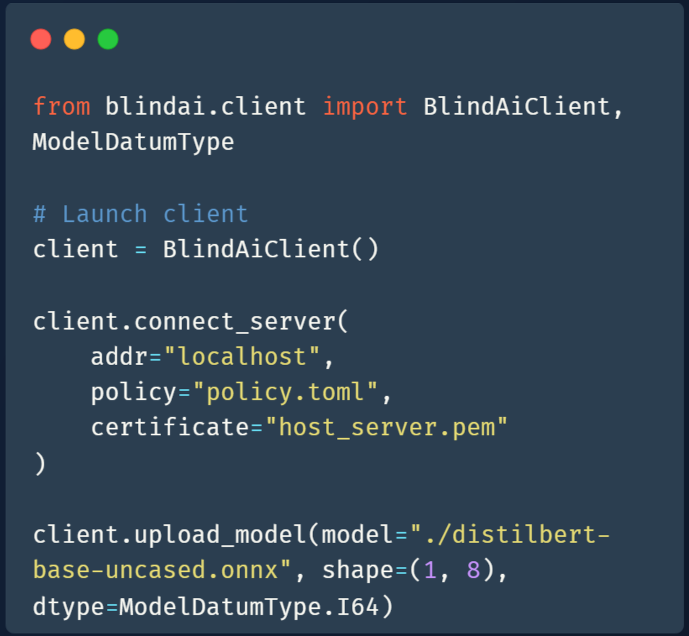
Cutting edge AI with privacy in 3 easy steps

1 Launch server



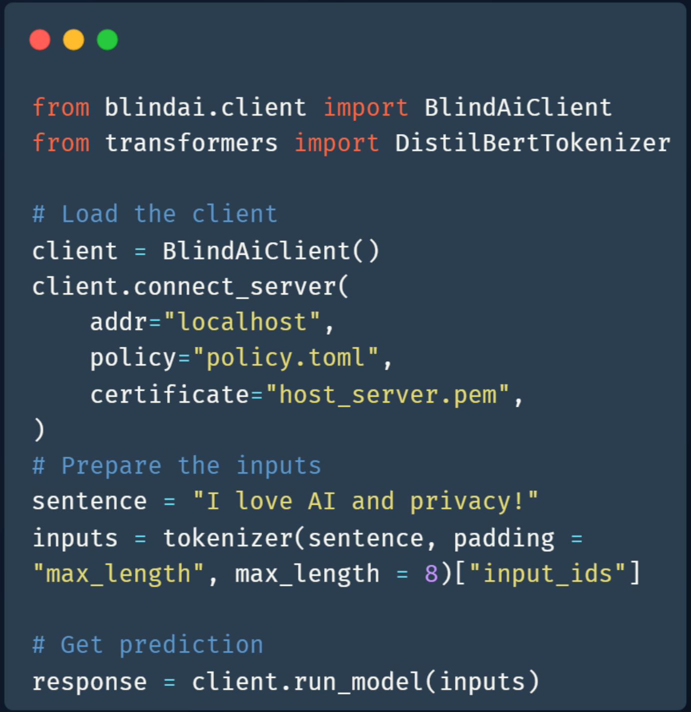
```
docker run \
    -p 50051:50051 \
    -p 50052:50052 \
    --device /dev/sgx/enclave \
    --device /dev/sgx/provision \
    mithrilsecuritysas/blindai-server:latest
/root/start.sh $PCCS_API_KEY
```

2 Upload model



```
from blindai.client import BlindAiClient,
ModelDatumType

# Launch client
client = BlindAiClient()

client.connect_server(
    addr="localhost",
    policy="policy.toml",
    certificate="host_server.pem"
)

client.upload_model(model="./distilbert-
base-uncased.onnx", shape=(1, 8),
dtype=ModelDatumType.I64)
```

3 Get prediction



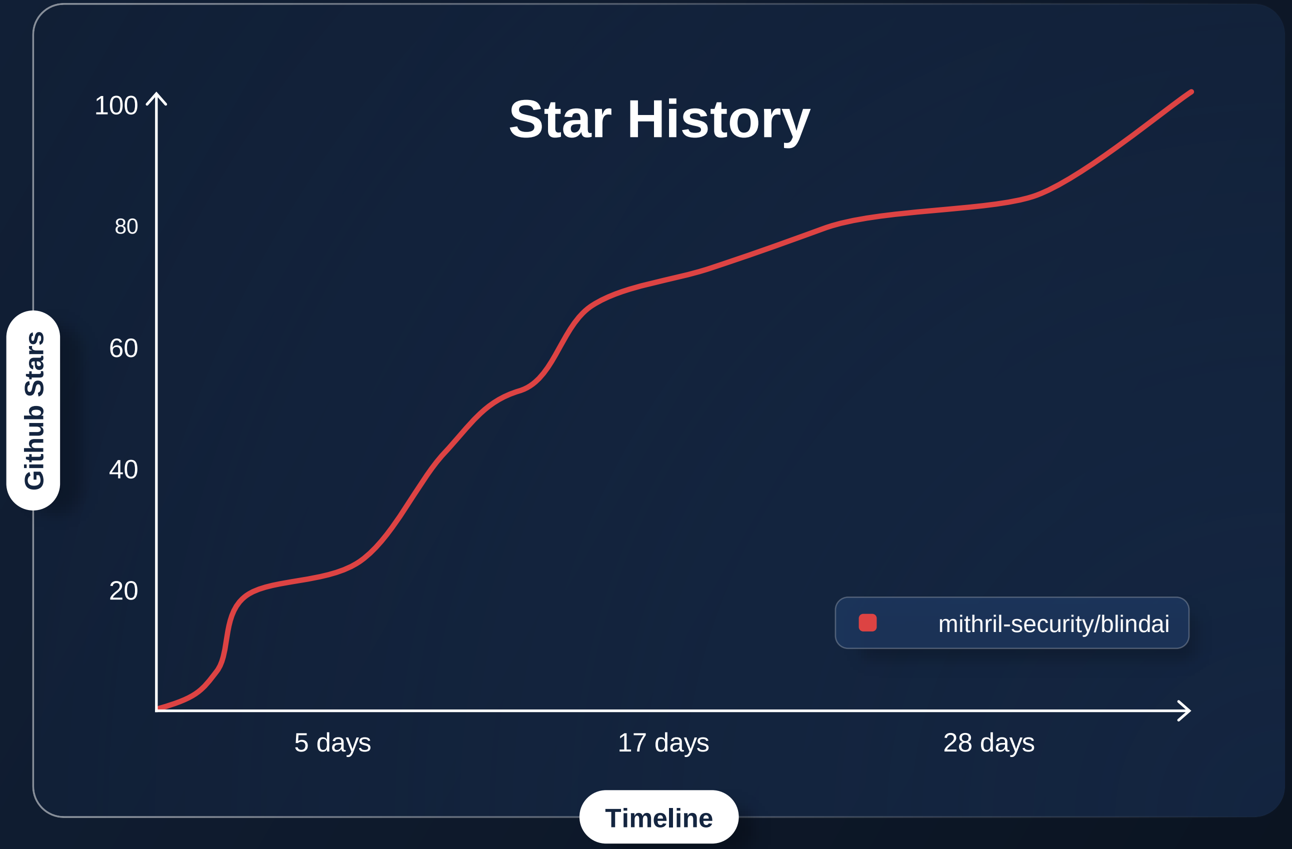
```
from blindai.client import BlindAiClient
from transformers import DistilBertTokenizer

# Load the client
client = BlindAiClient()
client.connect_server(
    addr="localhost",
    policy="policy.toml",
    certificate="host_server.pem",
)
# Prepare the inputs
sentence = "I love AI and privacy!"
inputs = tokenizer(sentence, padding =
"max_length", max_length = 8)["input_ids"]

# Get prediction
response = client.run_model(inputs)
```

MITHRIL SECURITY

Go-to-market:
Open-core for land grab

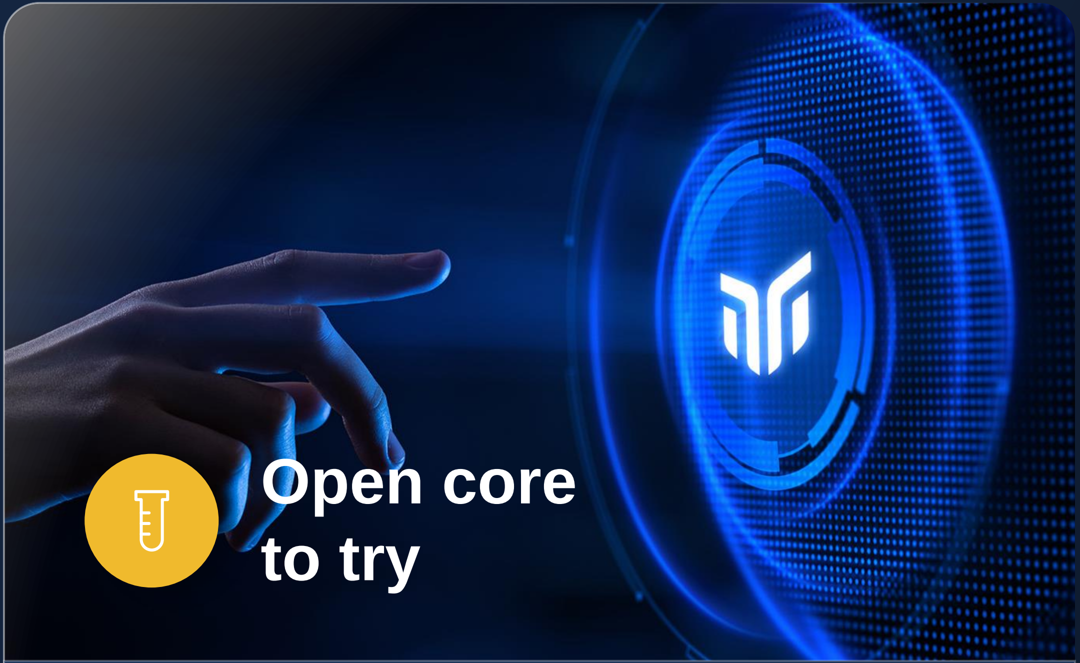
Better security

Faster adoption



MITHRIL SECURITY

Business model:
Open-core with Cloud platform



Open core to try

Cybersecurity features

Enterprise features to deploy

Acceleration - Cluster deployment - Managed Cloud

Our **Team**

Daniel

CEO

HEC PARIS Microsoft

Wrote articles on privacy ranked **#1 on Google**

Mehdi

CTO

42 Valeo

Built multi-channel detection **Covid-19 diagnostic** terminal

Raphaël

COO

WAVESTONE NEOMA

Led compliance analysis of banking projects for **cloud AI adoption**

Corentin

Head of Cybersecurity

INP ENSEEIHT EPFL

Experienced in **cybersecurity**, **and** passionate of **cryptography** and **PETs**

MITHRIL SECURITY

Our Advisors

Thomas Wolf

CSO
Hugging Face

CSO at Hugging Face
world expert in AI

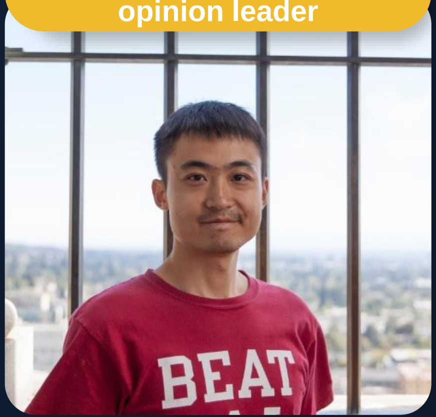
Tony Wasserman

Board director
Open-Source Initiative

Spent over 17 years teaching OS, 20 years as a **senior software executive**

Yu Ding

Confidential Computing opinion leader



Over 20 publications on CC, **Rust SGX initiative lead**

John Hughes

General partner
Swift Ventures

SWIFT VENTURES

Previously VP of Product and Engineering at Adobe
Co-founder at TubeMogul (IPO)

MITHRIL SECURITY

We are raising $1.4M

to become the open-source leader for confidential AI within 18 months

Objectives

2,500

GitHub stars

AI community traction

$1M

ARR

Clients' traction