IAM Was Built For Humans
- AI Agents didn't get the memo

Jacob Ideskog – CTO @ Curity

CURITY

71%

CURITY®


Robots
2FA

The Original **IAM Model**

Traditional IAM assumes:

- A human user
- A browser
- A login

CURITY®

~~Who is the user?~~

CURITY®

What does this app need to know to safely grant access?

CURITY®

Application-Centric Identity

CURITY®

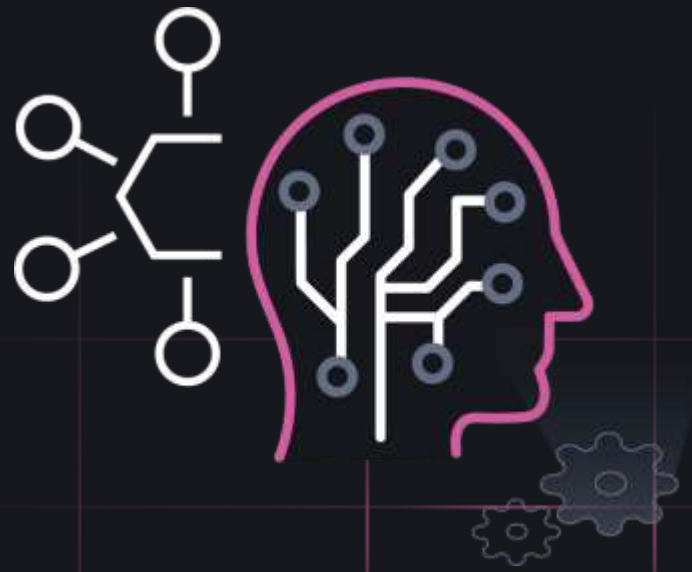
- Customer Services
  - Accounts
  - Preferences
  - PII & Consent
- Commerce
  - Payments
  - Pricing & promotions
  - Orders & Transactions
- Stores
  - Store Registers
  - Supply chain

CURITY®

Agents Change the Shape of Access

Agentic systems:

- Act autonomously
- Trigger actions via events
- Call tools and APIs dynamically



They amplify existing API access patterns

Most TOOLS are APIs

CURITY®

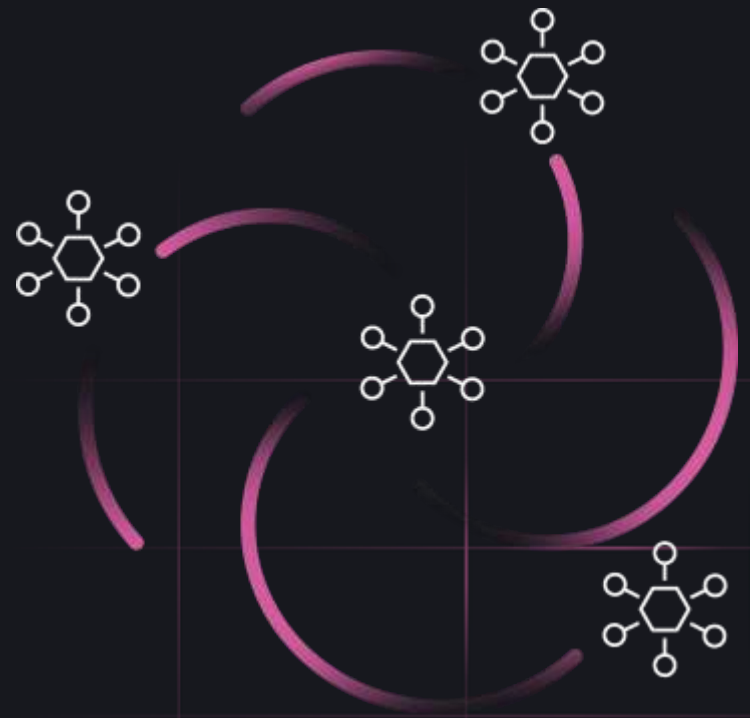
APIs are the Data Plane – Identity the Control Plane

APIs are where access actually happens

They connect:

- Applications
- Services
- Agents and AI components

Identity must operate at the API layer



CURITY®

Agents Require Token Intelligence

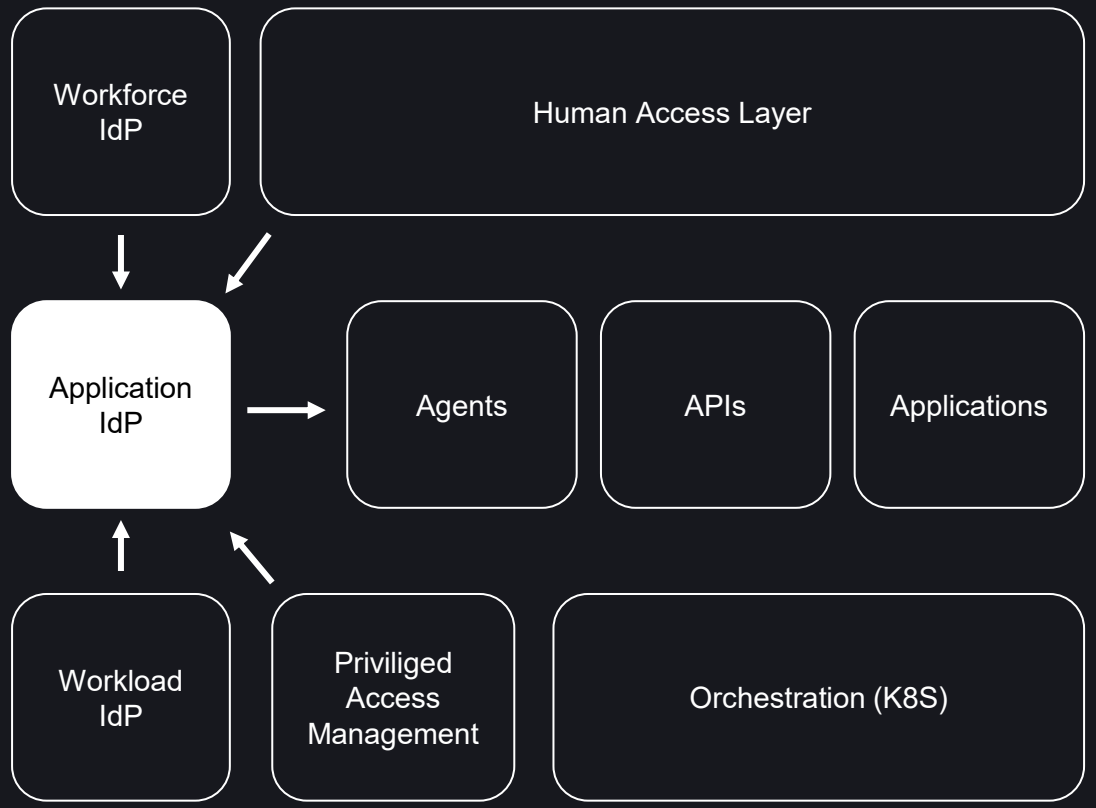
Tokens should be dynamically issued and based on:

- agent identity
- context
- policy
- time and risk

Tokens are short lived (JEP/JIT)

CURITY®

Token Intelligence for JEP/JIT



Identity and Access are not the same

Application Centric Identity Needs to

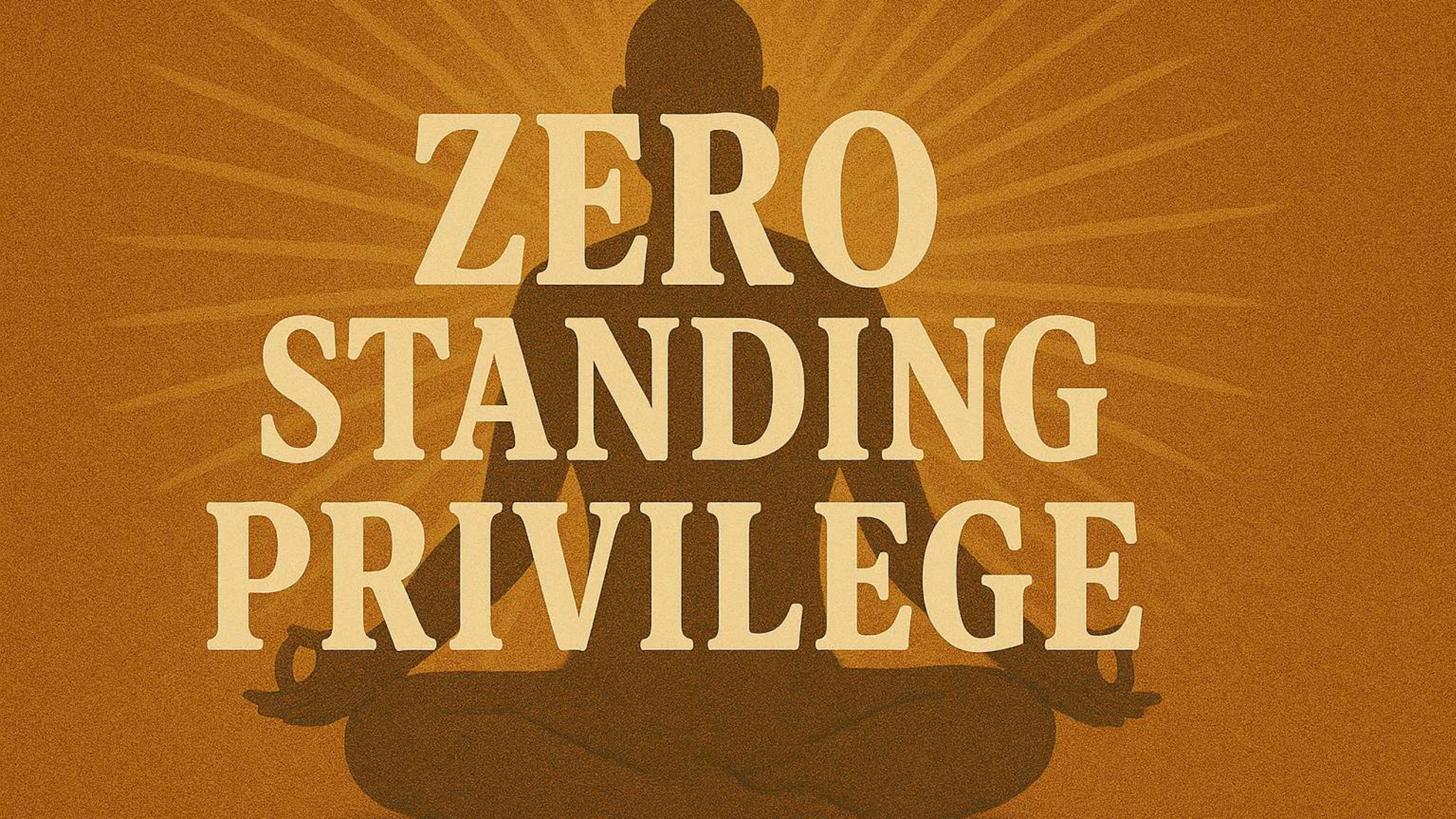
- Bridge workload identities with access
- Dynamically adapt access based on context (JEP/JIT)
- Discover and manage intent
- Policy based issuance

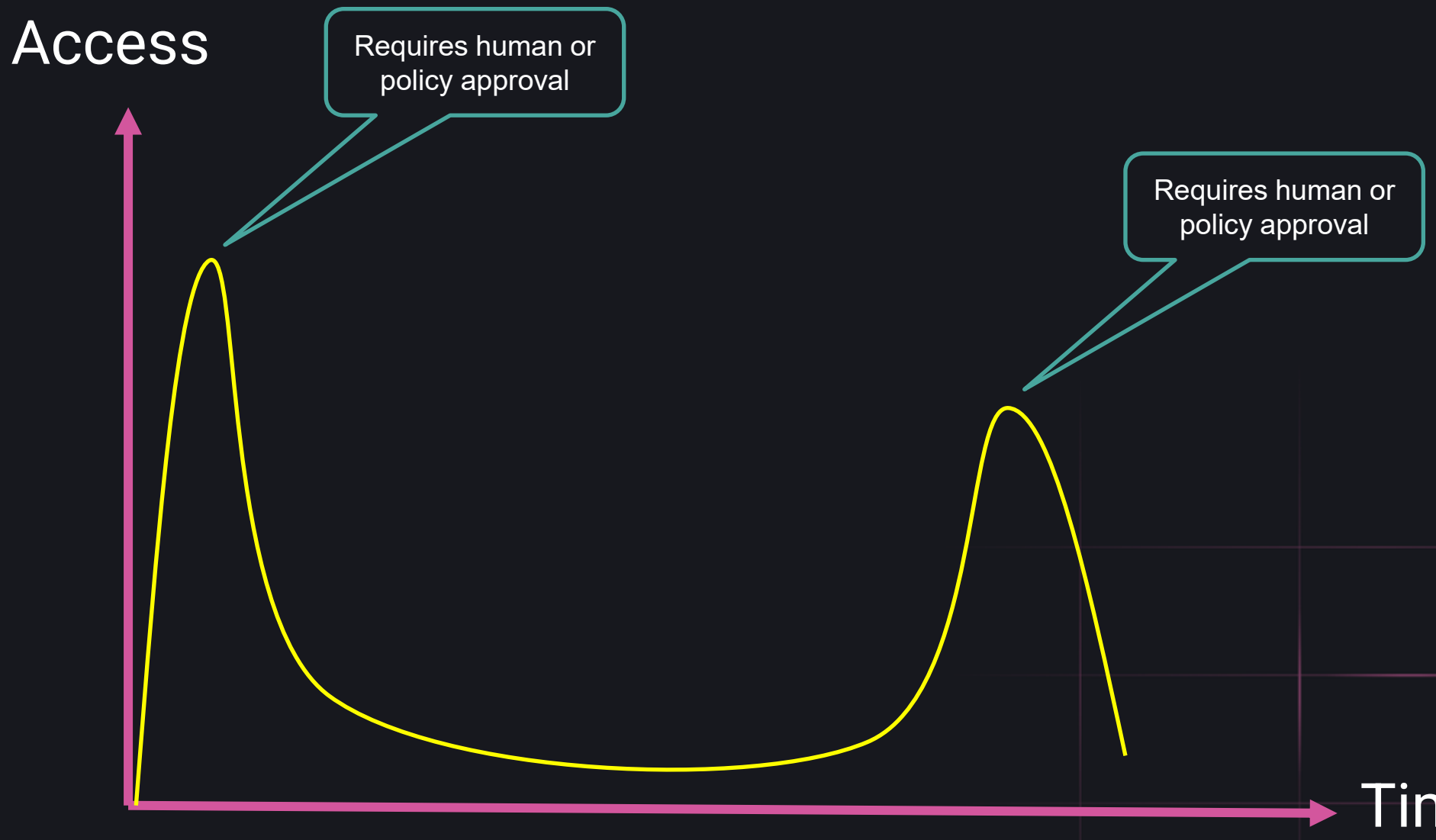
CURITY®

They’re…
autonomous

…and…
non-deterministic

least privilege


ZERO
STANDING
PRIVILEGE


Access
Requires human or policy approval
Requires human or policy approval
Time

CURITY®

Token Intelligence solves Zero Standing Privilege

JEP/JIT tokens are short lived

Access scope is re-evaluated on each issuance

No static credentials floating around

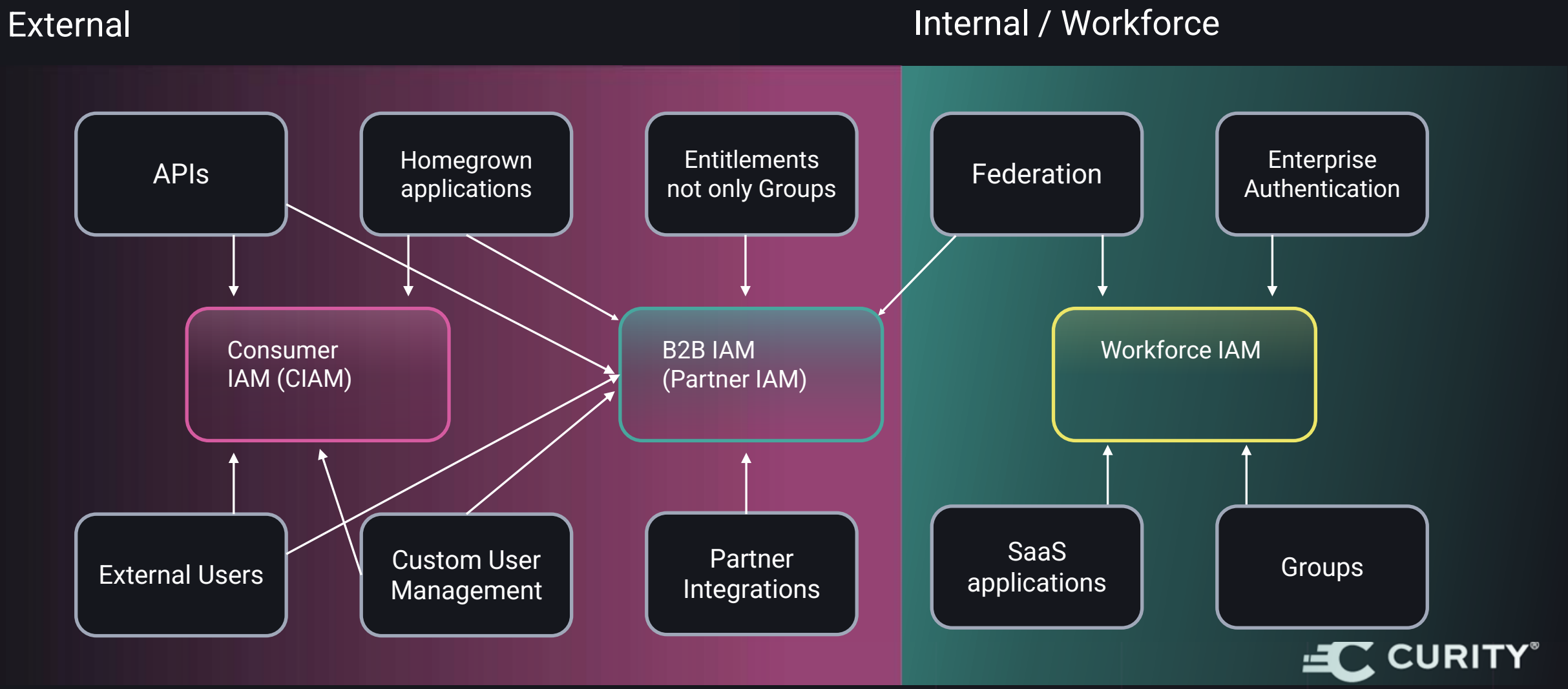
CURITY®

CURITY®

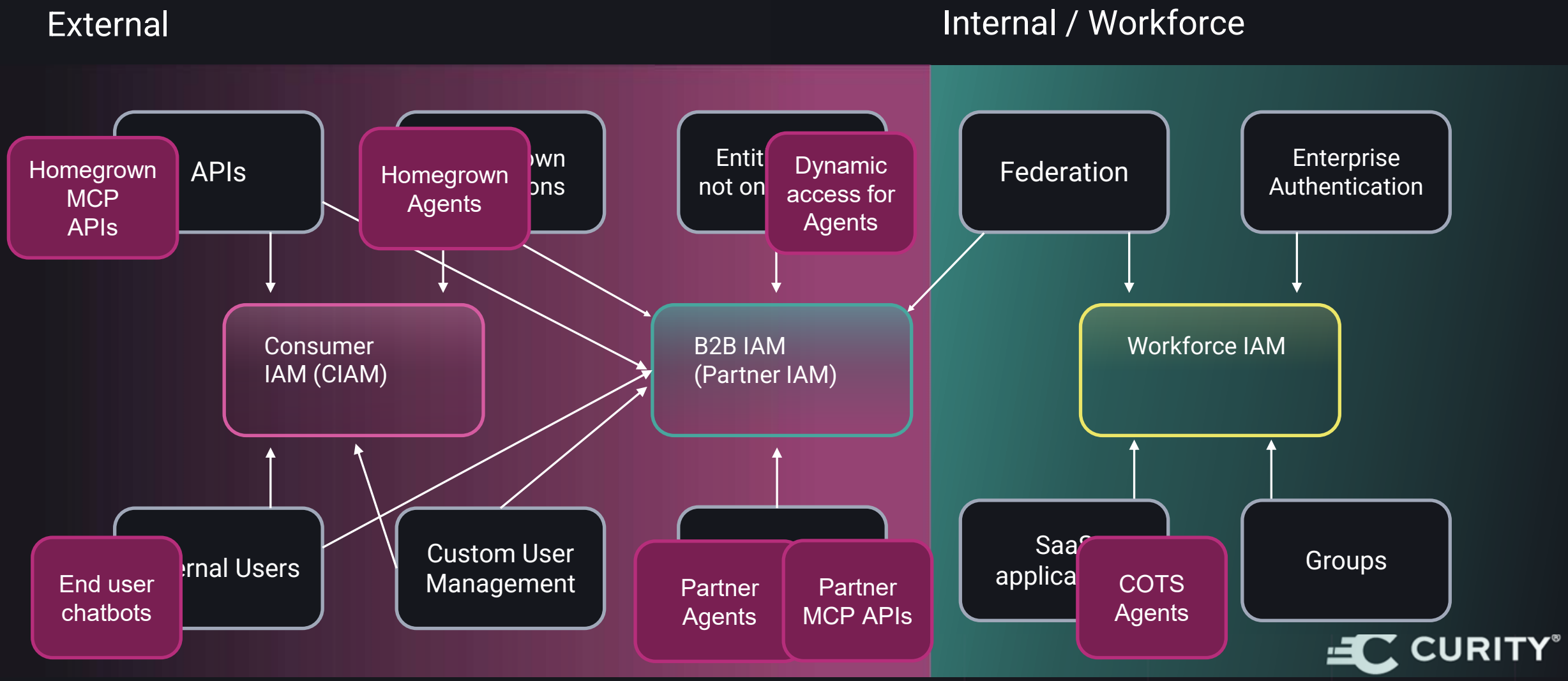
CIAM is dead
Long live applications

CURITY®

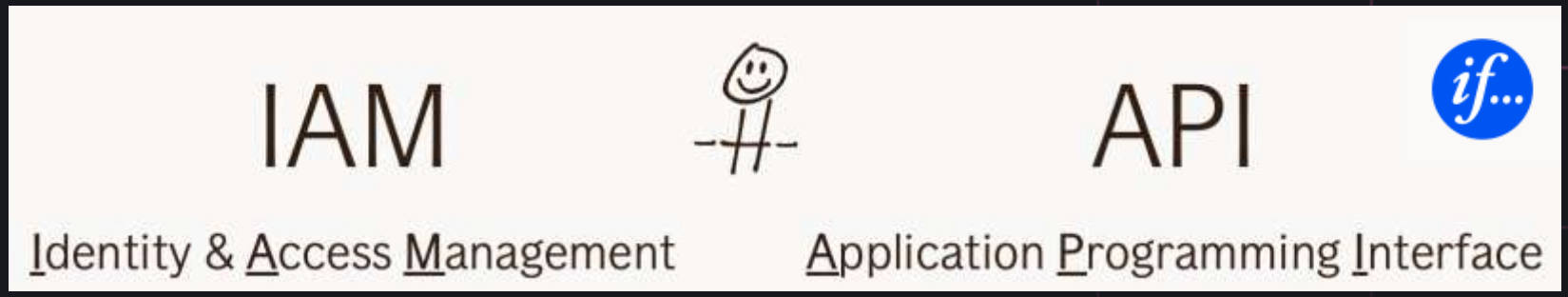
External vs Internal/Workforce IAM



External vs Internal/Workforce IAM



Workforce IAM → External IAM → API IAM



CURITY®

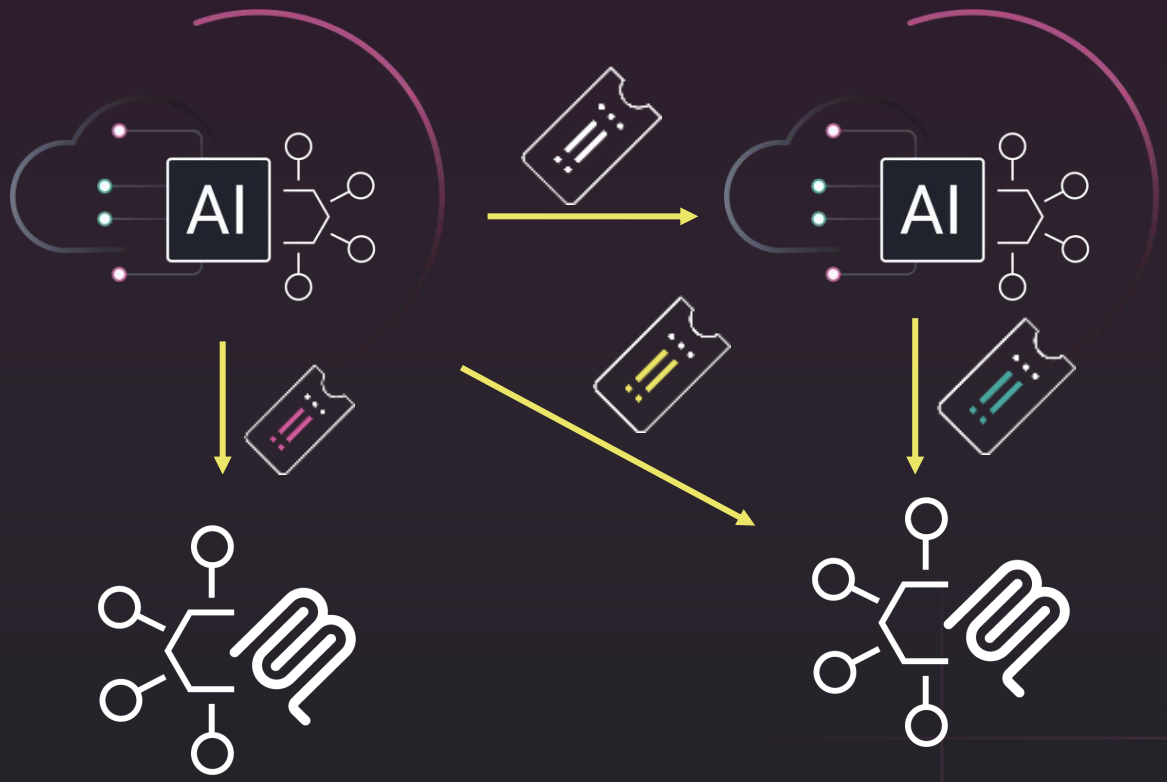
System User

Real User

CURITY®

we used to be the subject
now we are the context

move from thinking “users” to “access”



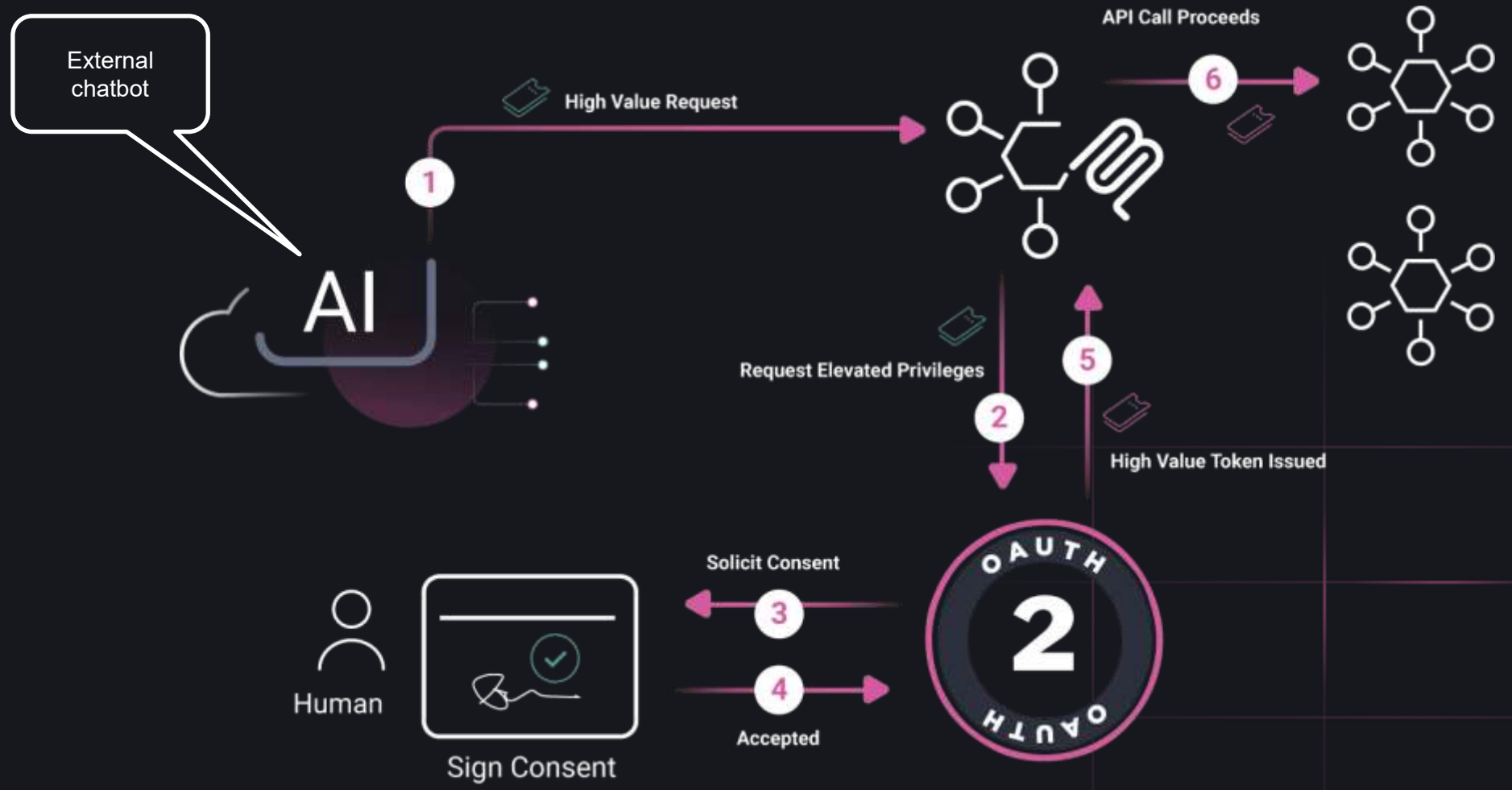
Token Intelligence brokers access

CURITY®

access is no longer an internal issue (pro tip: it never was)

CURITY®

User Consent



CURITY®

pace

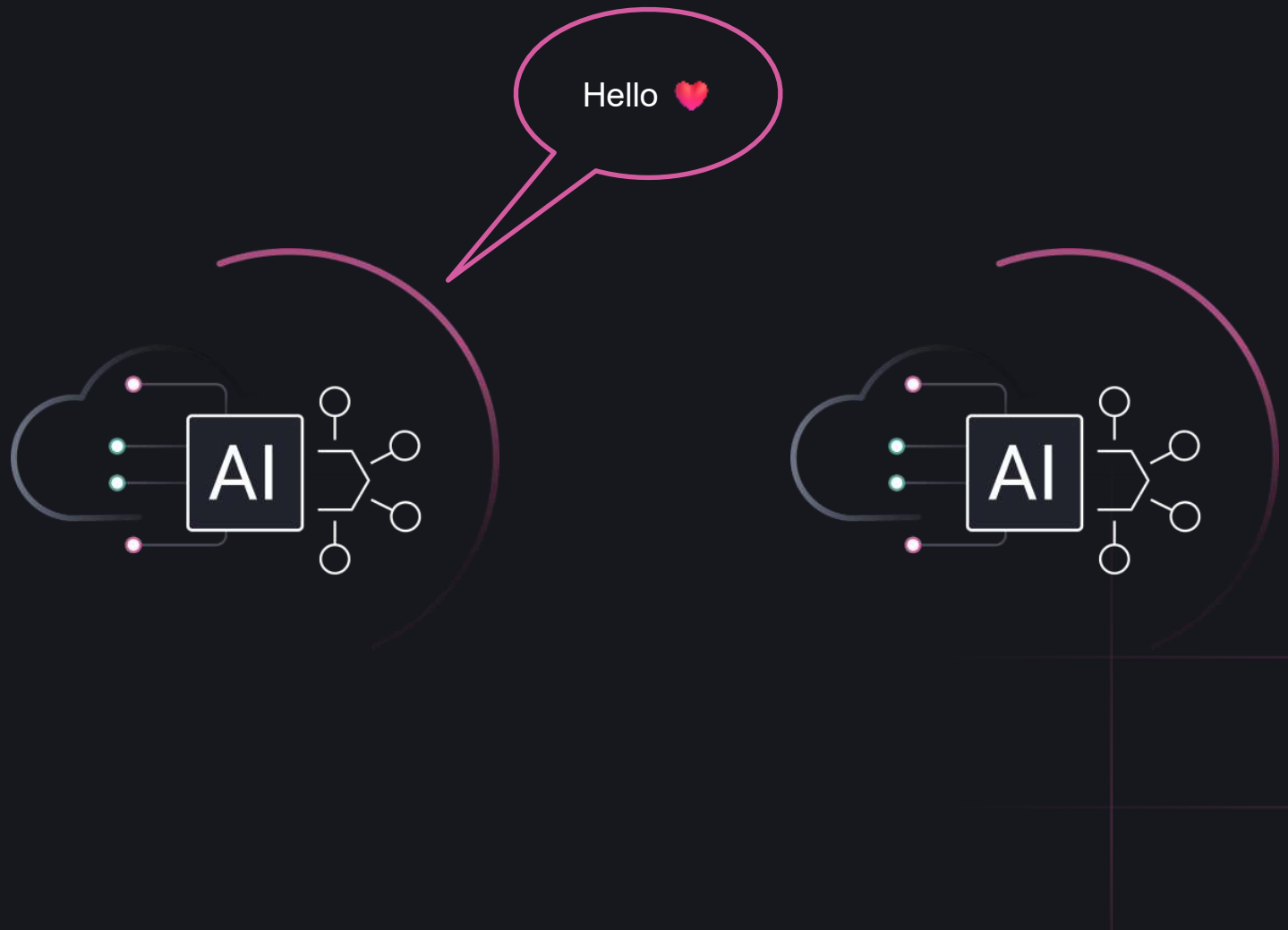
CURITY®

CURITY®

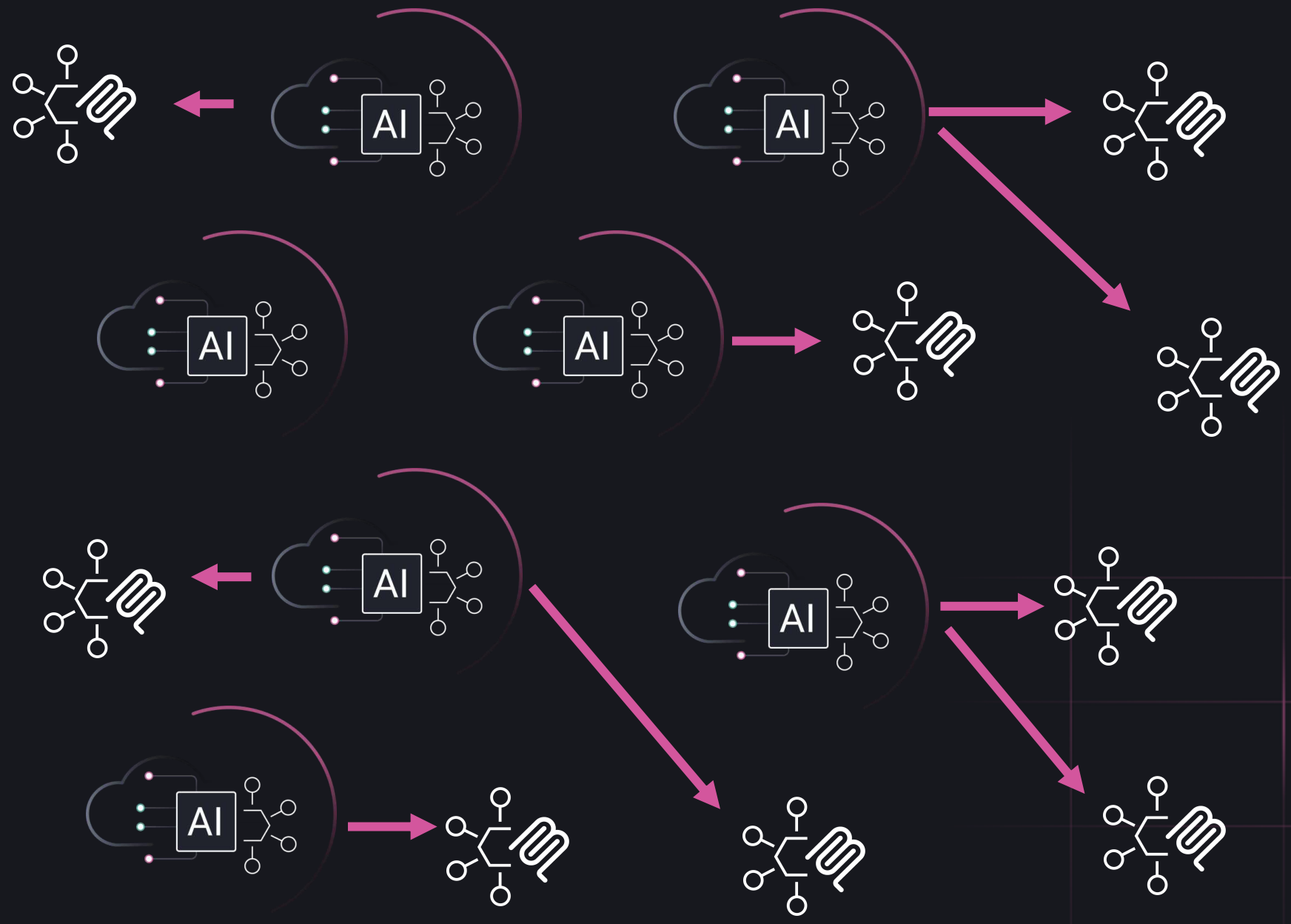
Keep control on the API side
So you can trust the agent

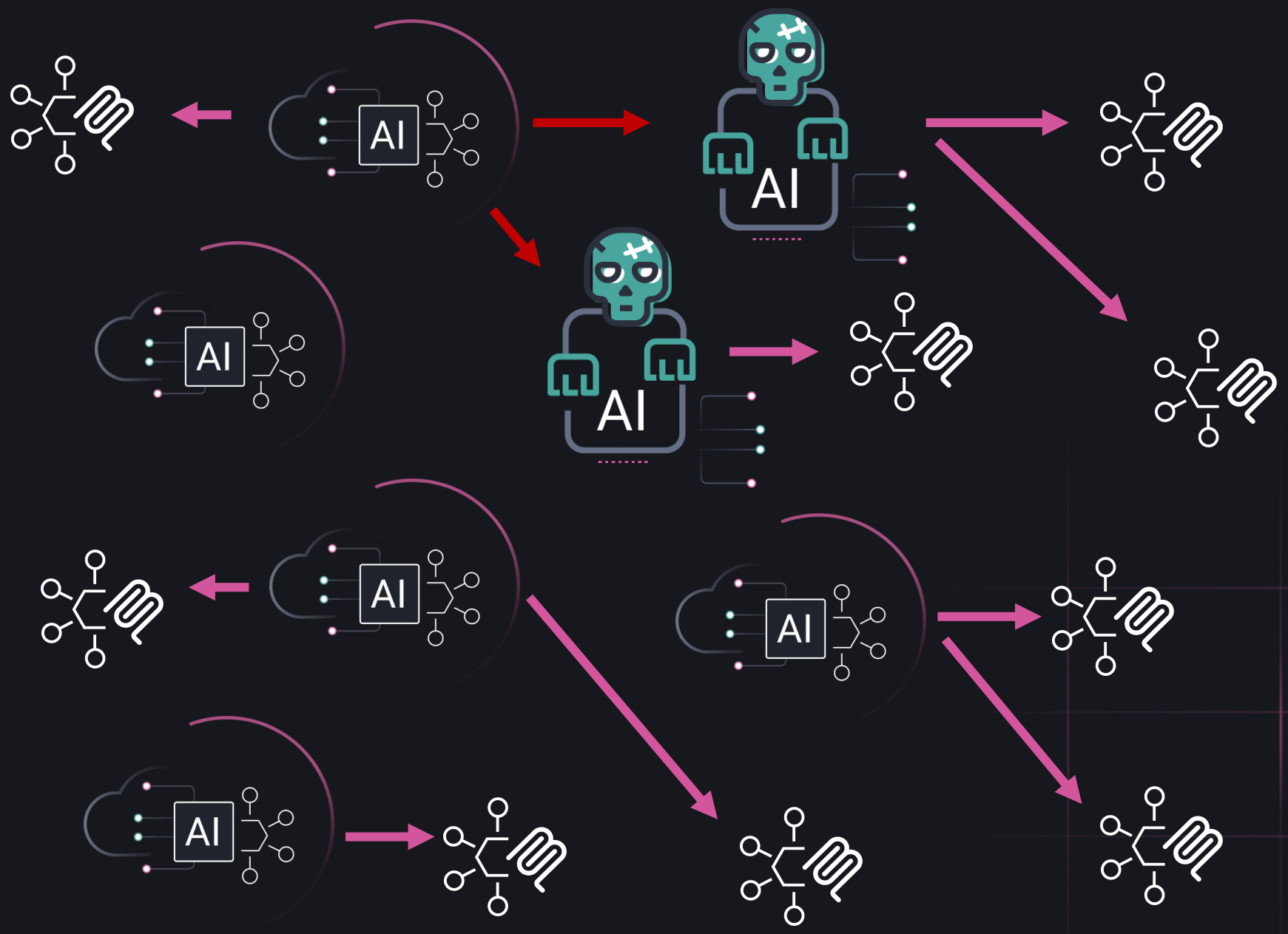
CURITY®


Zombies



CURITY®

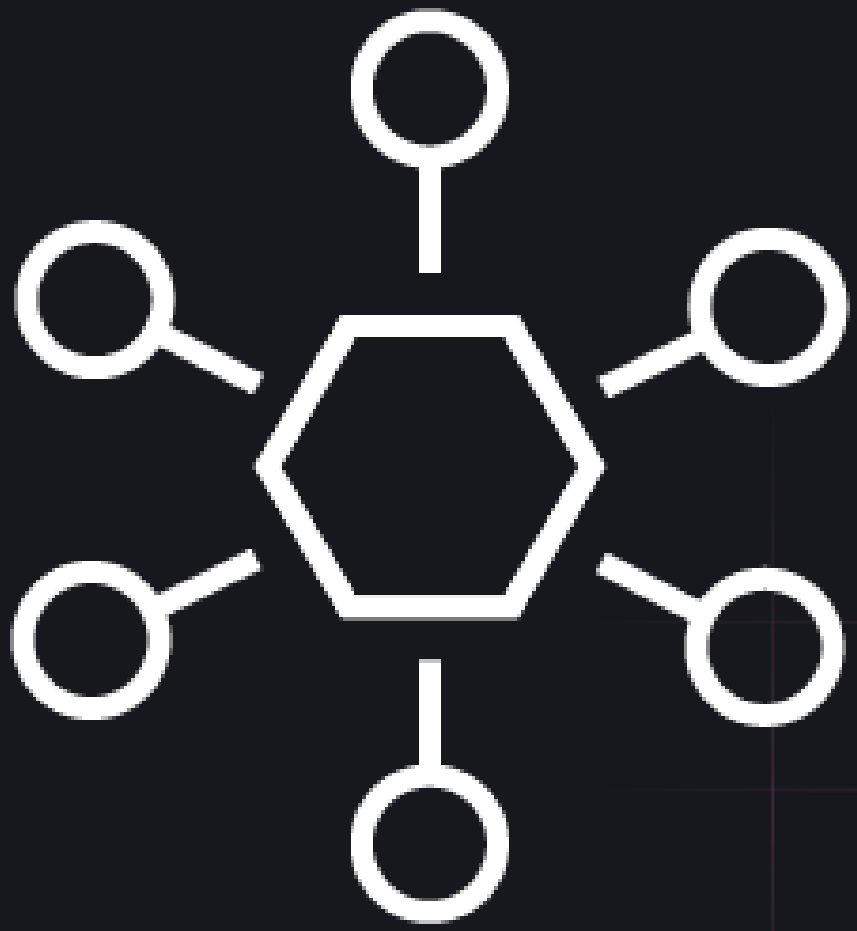

AI
AI
AI
AI
AI
AI
CURITY®



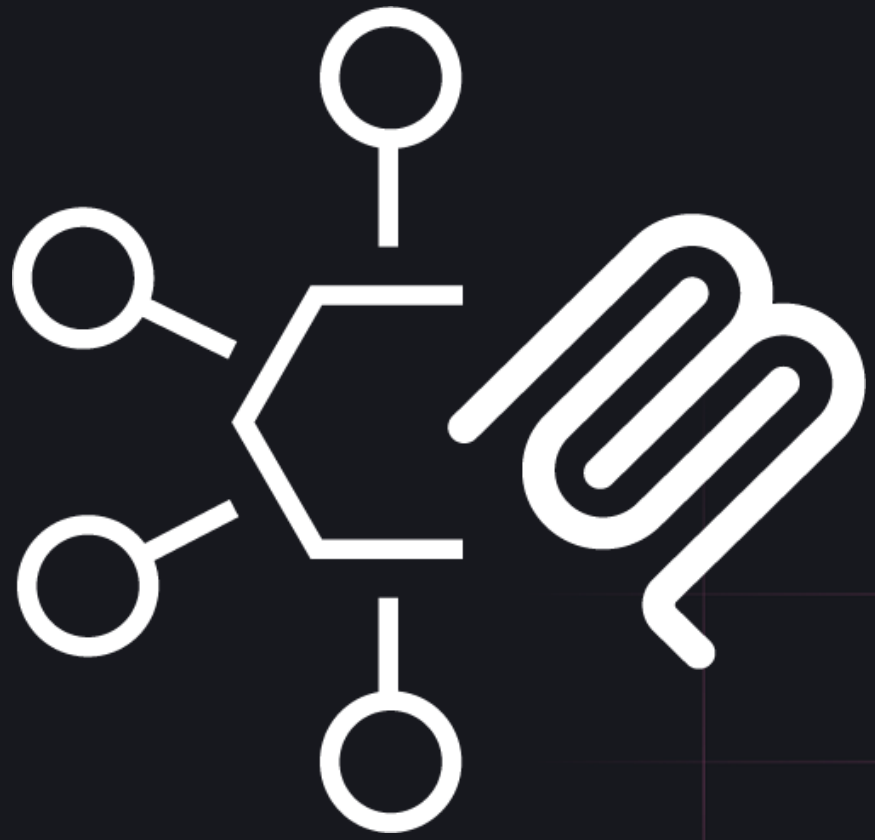
CURITY®

Oh sh*t!

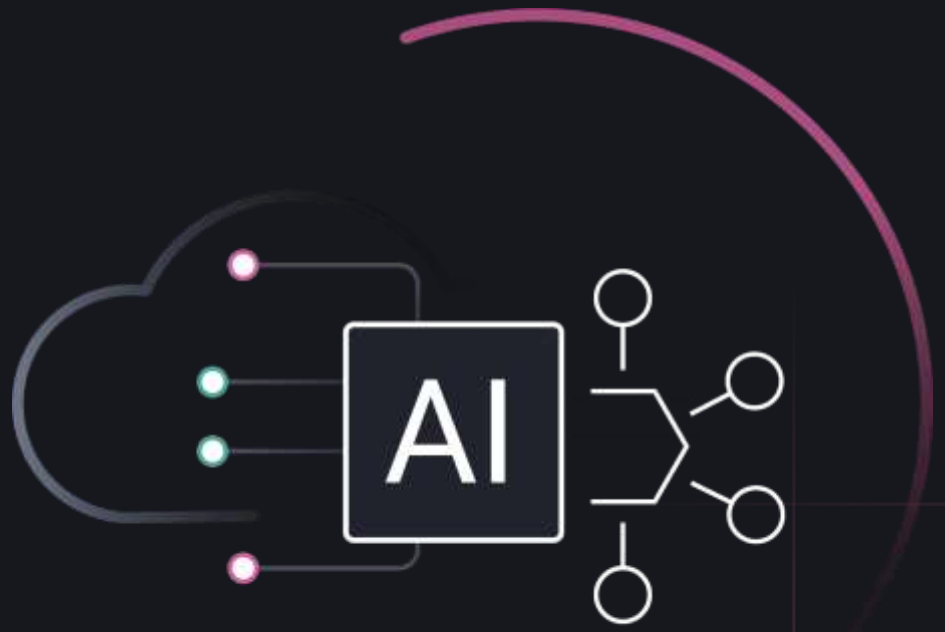

MOLTBOOK
MOLTBOOK
MOLTBOOK
MOLTBOOK



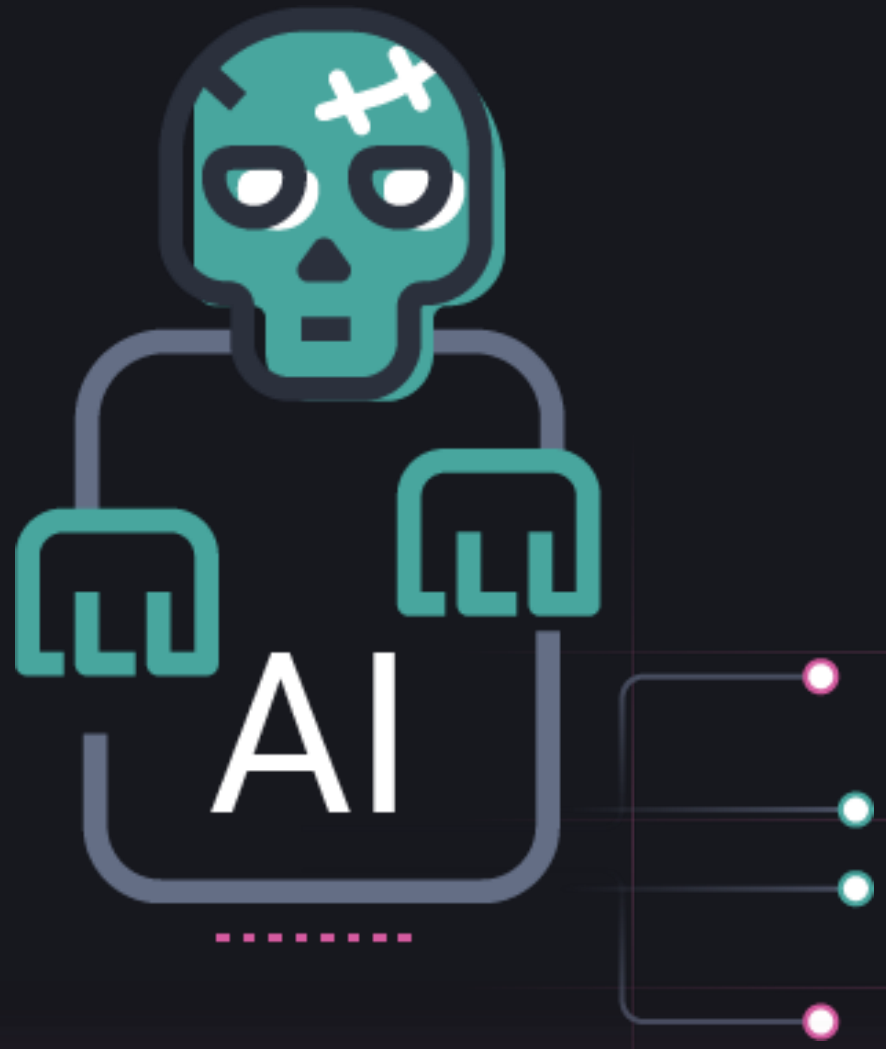
CURITY®



CURITY®



CURITY®



CURITY®

99.9%

CURITY®

Start preparations now

Add Token Intelligence

Keep control on the API side

Model Access for Application needs not Users

Design API First

Beware of the zombies

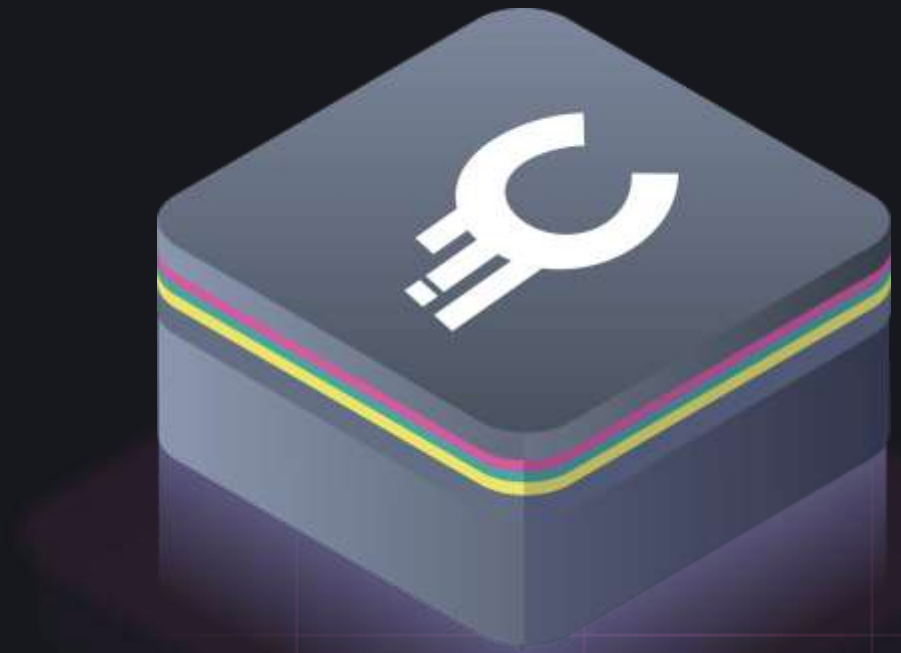
CURITY®

Thank You!

curity.io

developer.curity.io

info@curity.io



CURITY®