

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

Jacob Ideskog – CTO @ Curity

<API>



71%



Robots

The Original IAM Model



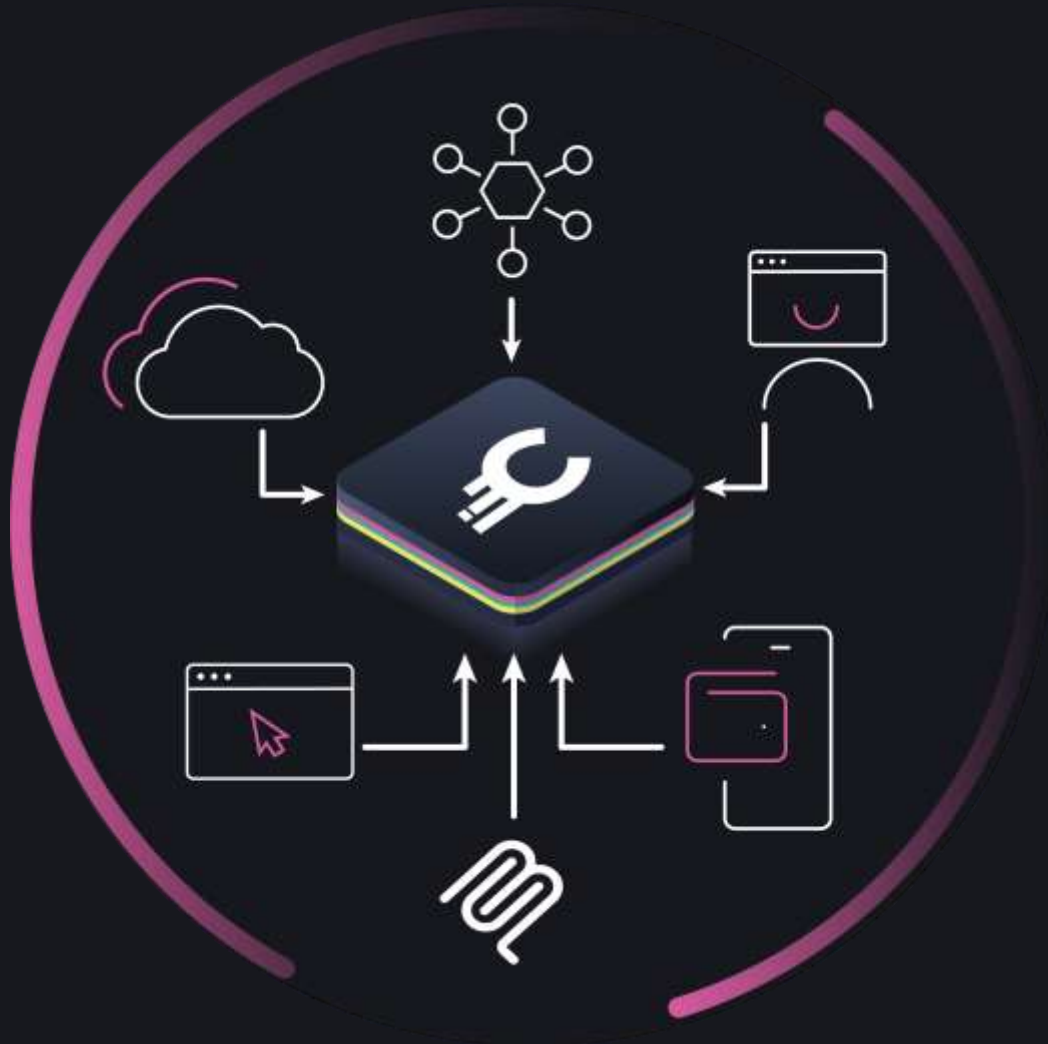
Traditional IAM assumes:

- A human user
- A browser
- A login

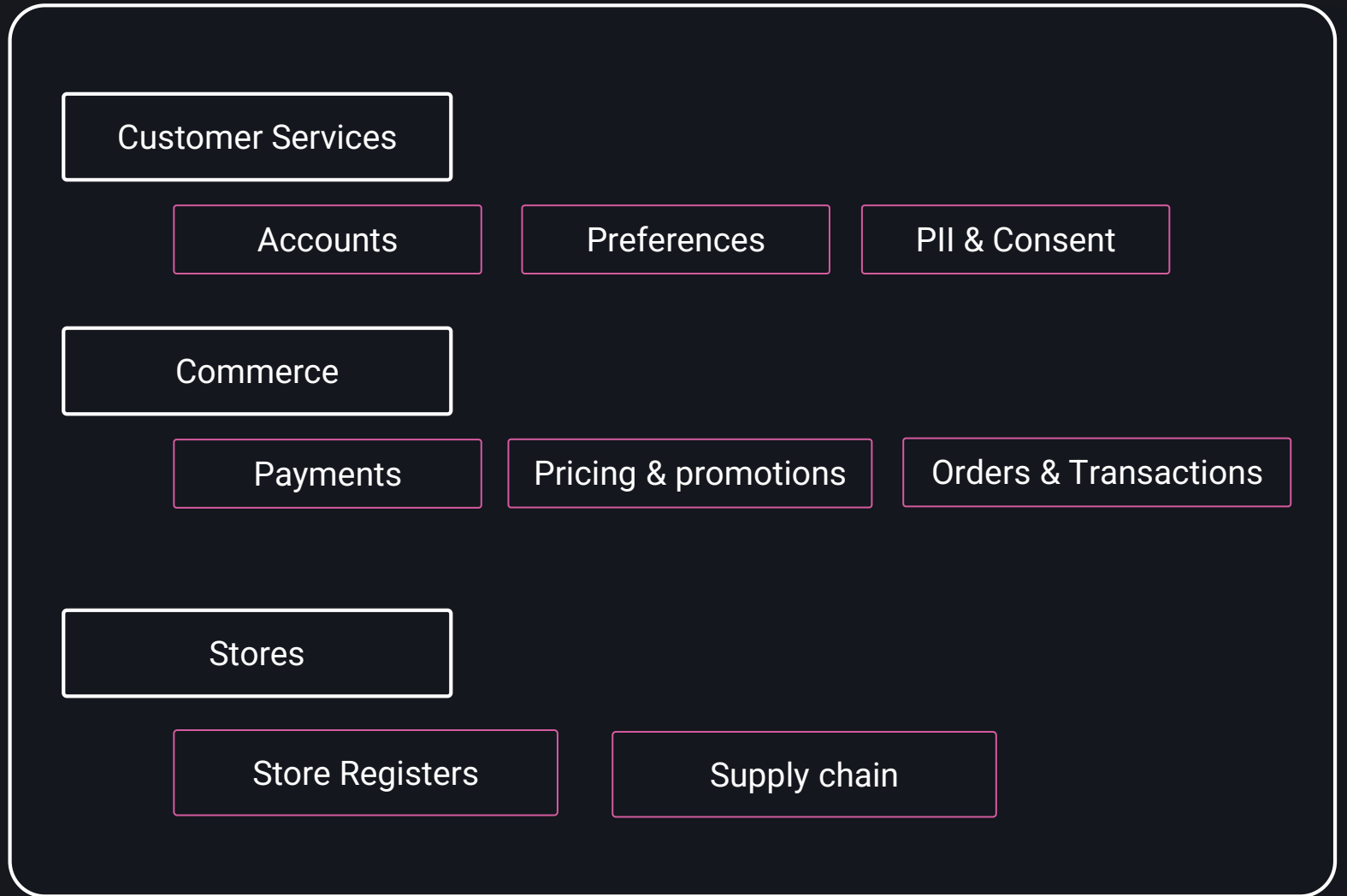
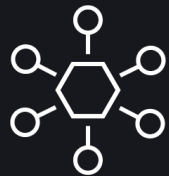
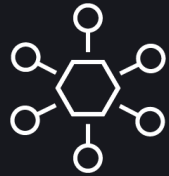
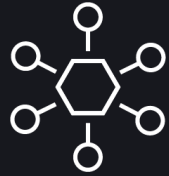
~~Who is the user?~~

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





Application-Centric Identity



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



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



Agents Require Token Intelligence

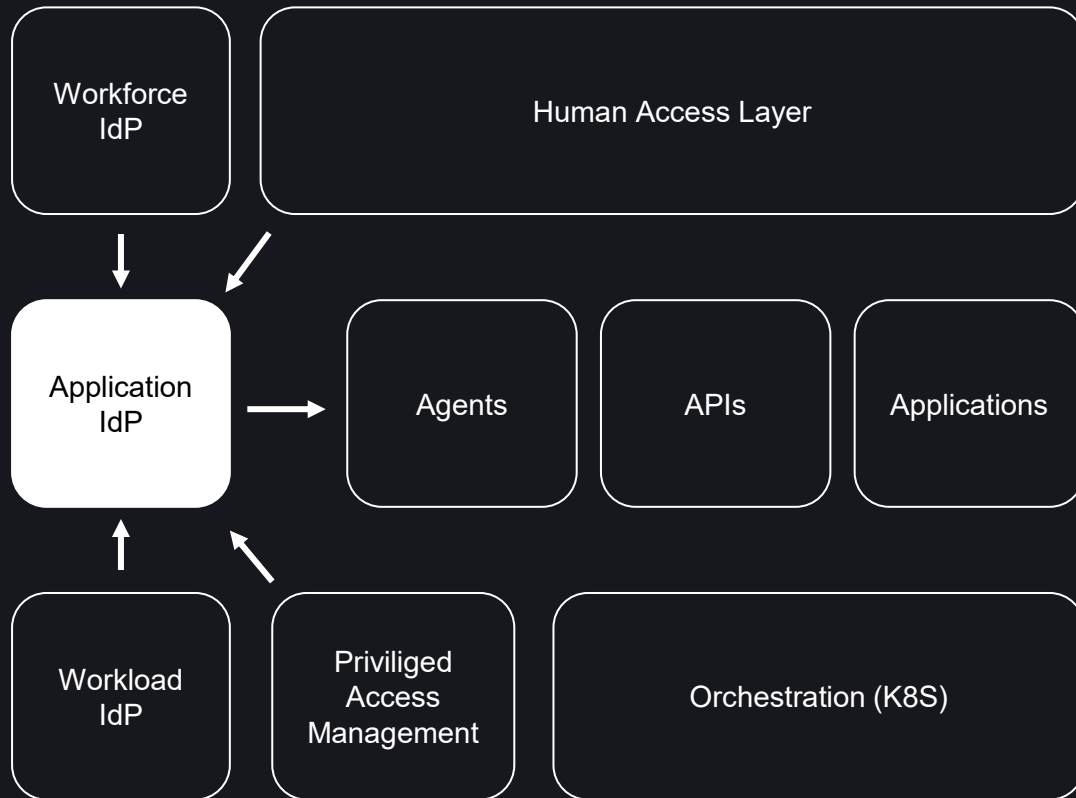


Tokens should be dynamically issued and based on:

- agent identity
- context
- policy
- time and risk

Tokens are short lived (JEP/JIT)

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

**They're...
autonomous**

**...and...
non-deterministic**

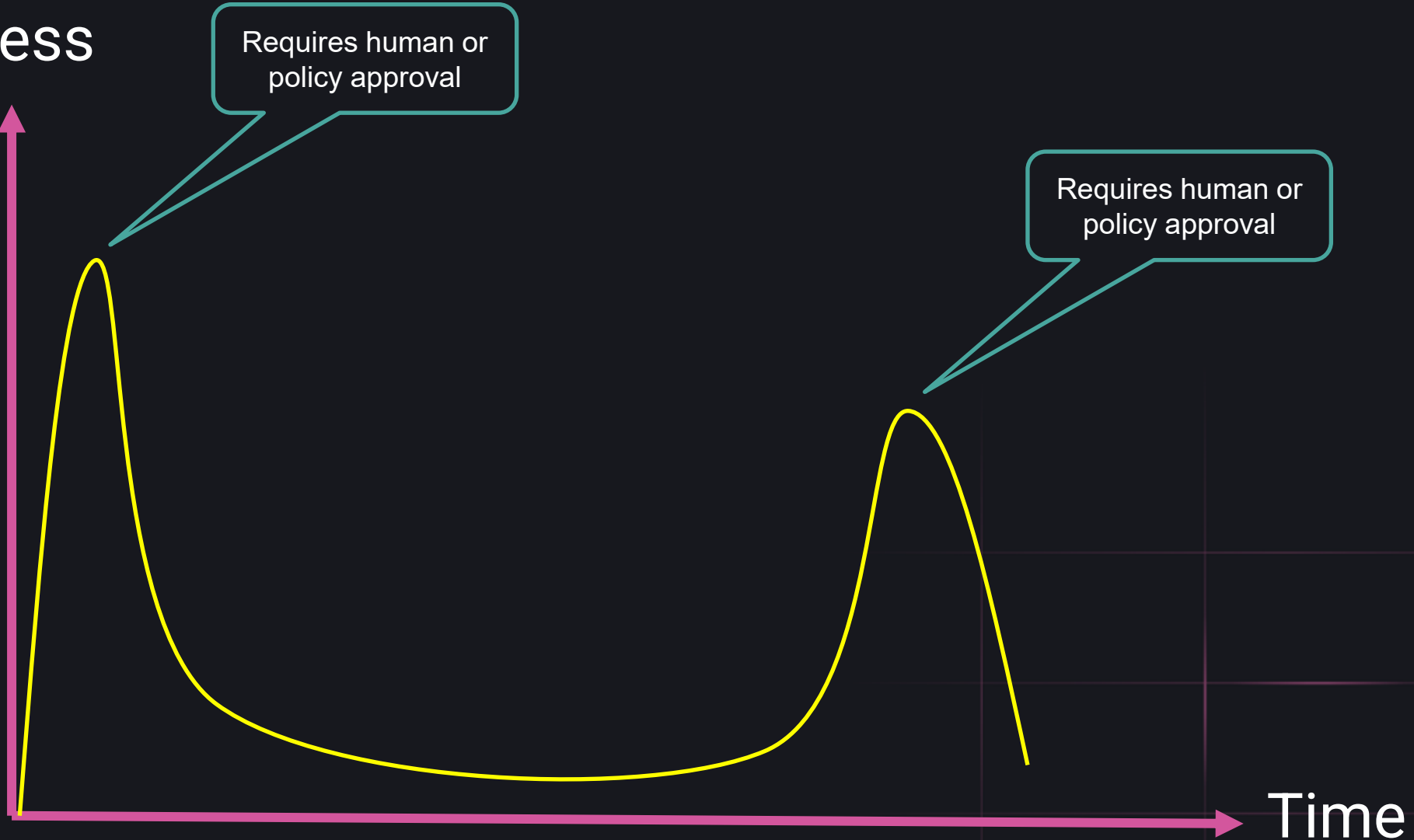


least privilege

The background features a dark brown silhouette of a person in a meditative pose, with hands resting on their knees. Behind the silhouette is a sunburst pattern of radiating lines. The overall color palette is warm, consisting of various shades of brown and tan.

ZERO STANDING PRIVILEGE

Access



Time

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

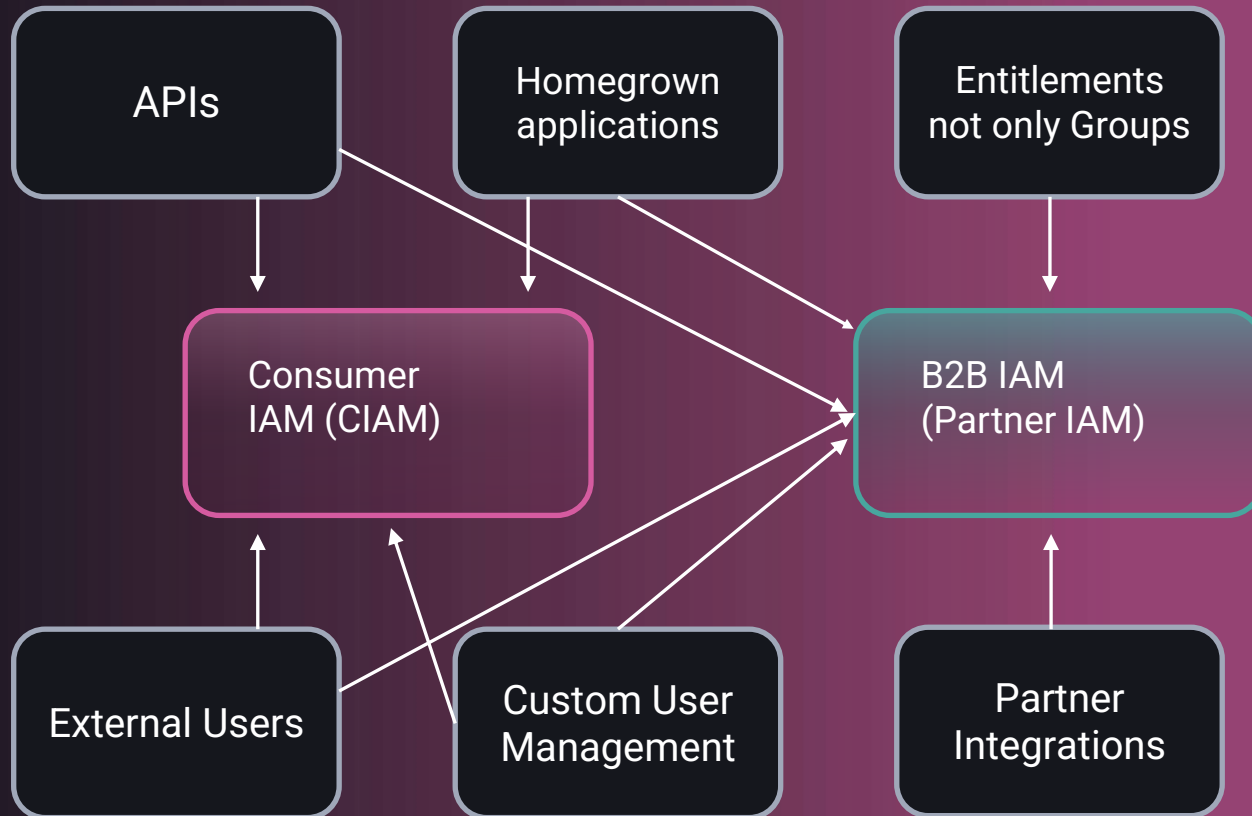




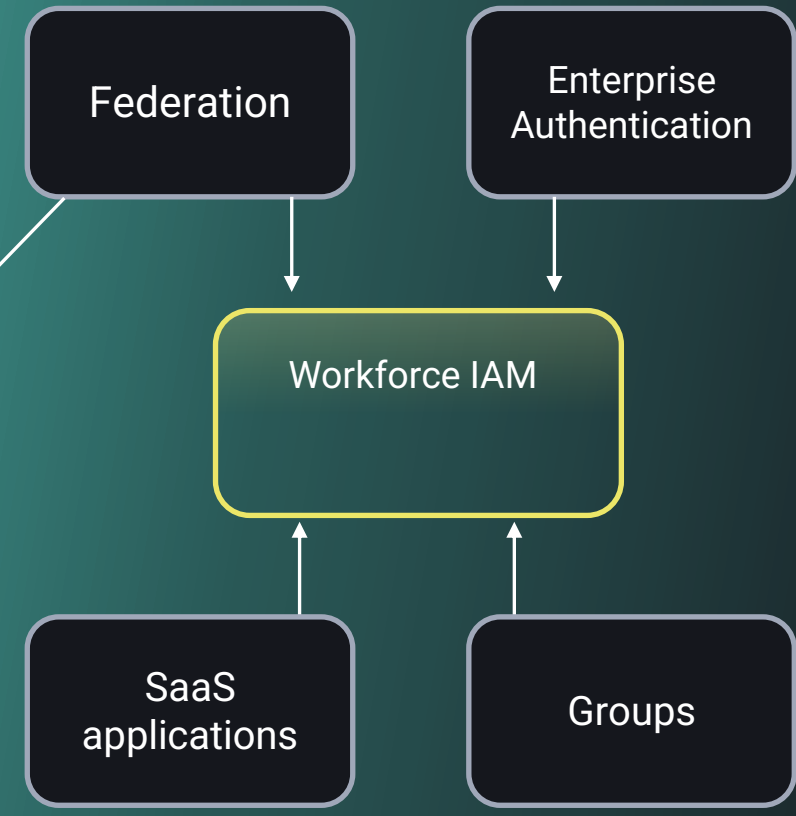
CIAM is dead
Long live applications

External vs Internal/Workforce IAM

External

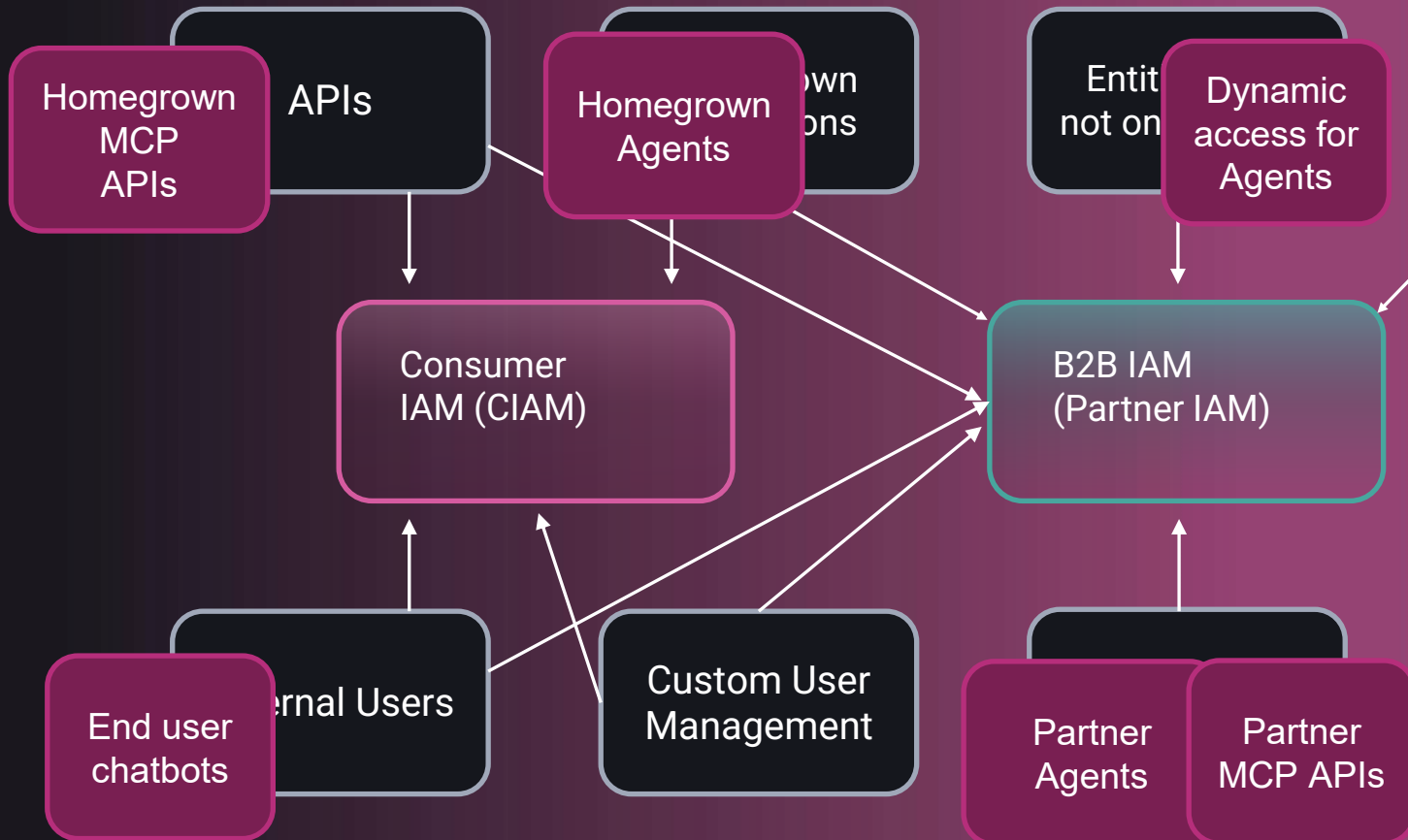


Internal / Workforce

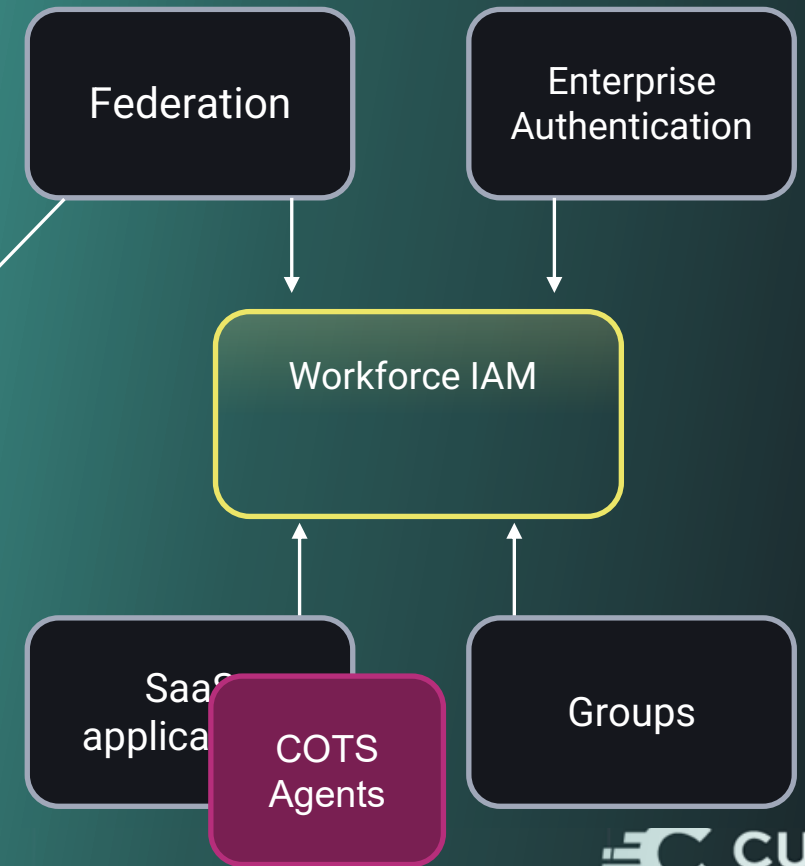


External vs Internal/Workforce IAM

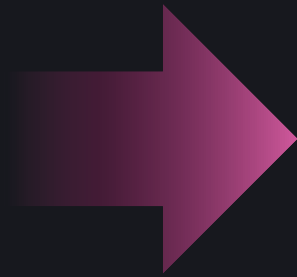
External



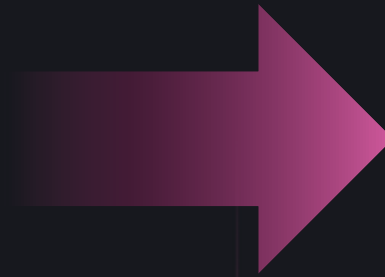
Internal / Workforce



**Workforce
IAM**



**External
IAM**



**API
IAM**

IAM



API



Identity & Access Management

Application Programming Interface



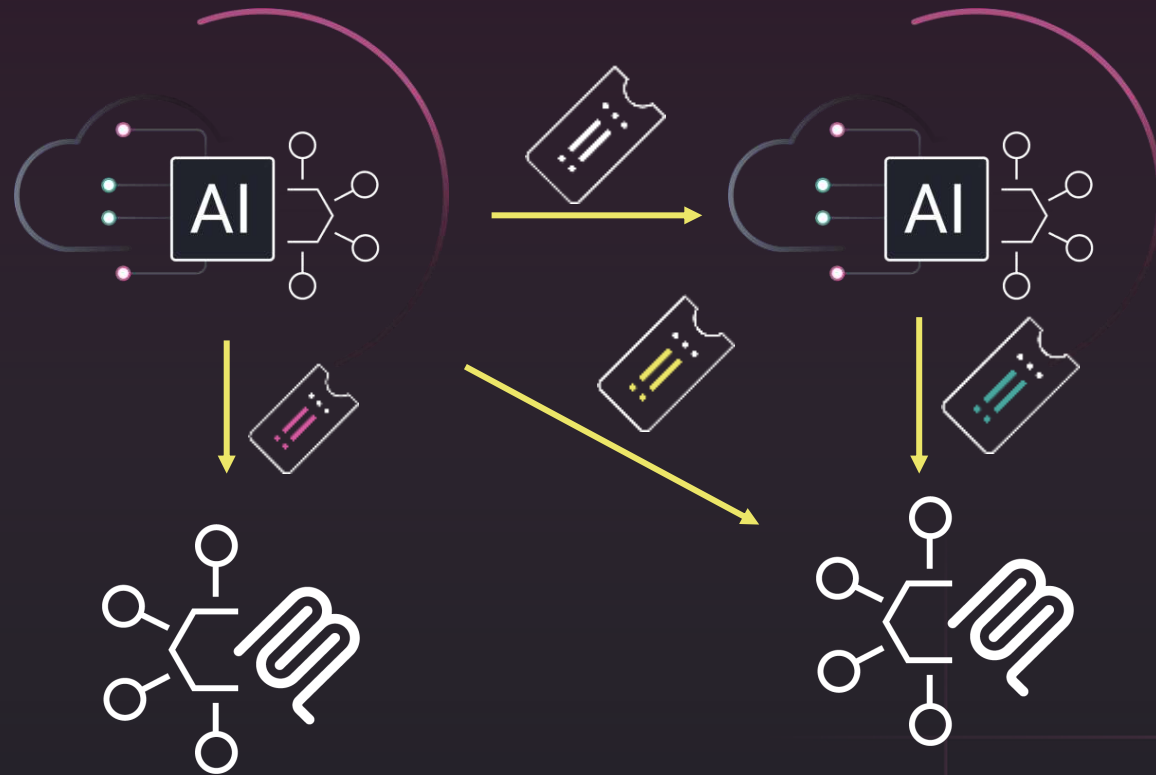
System User



Real User

**we used to be the subject
now we are the context**

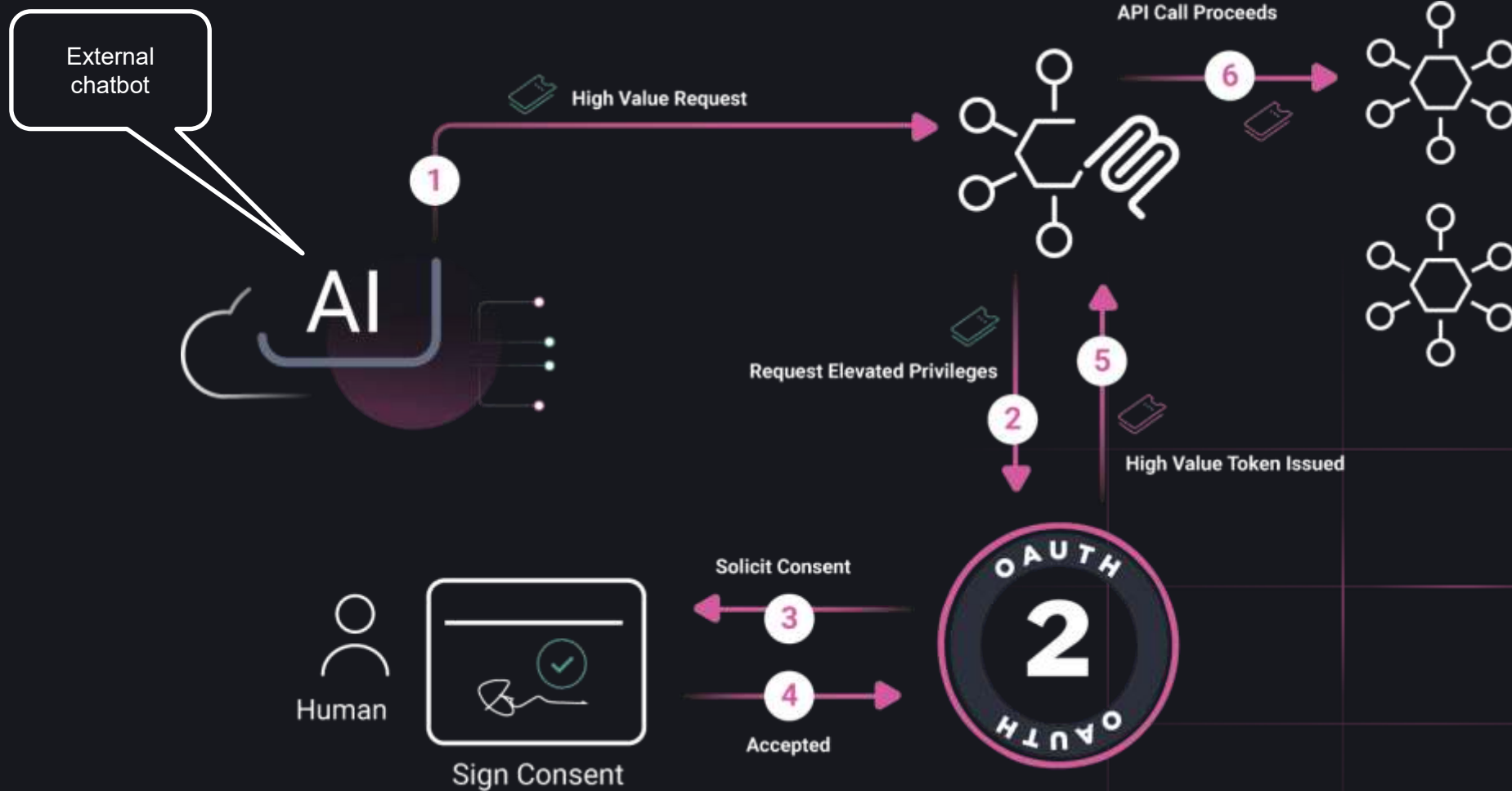
**move from thinking “users”
to “access”**



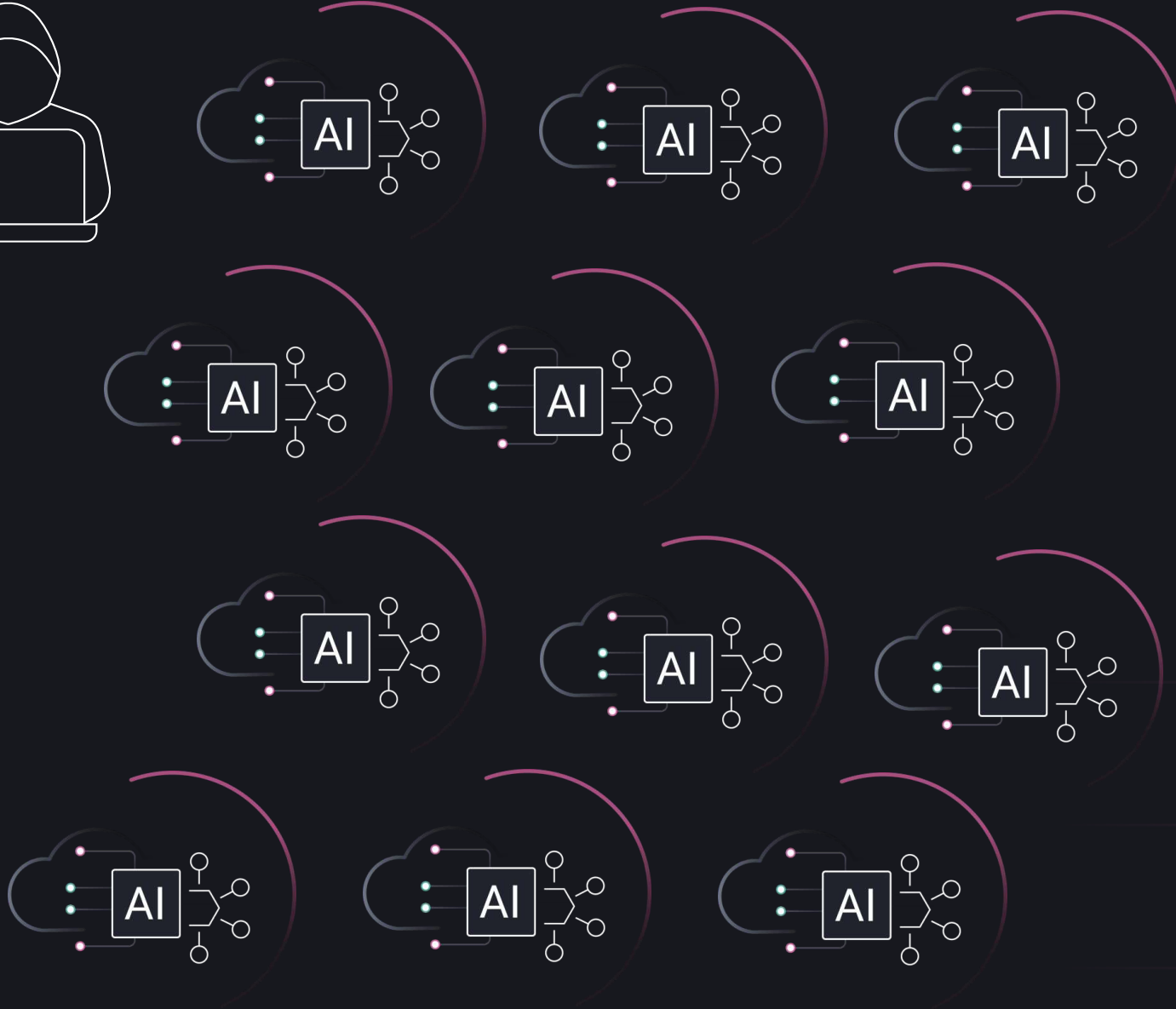
Token Intelligence brokers access

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

User Consent



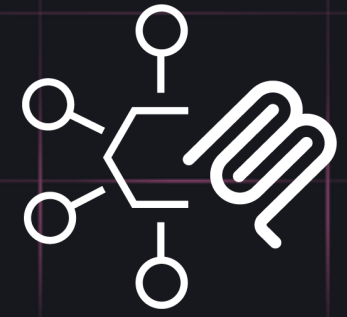
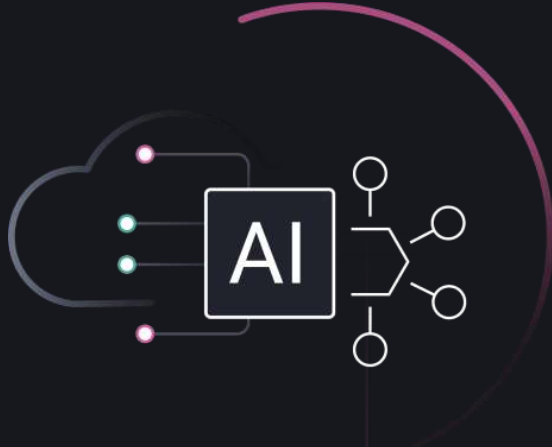
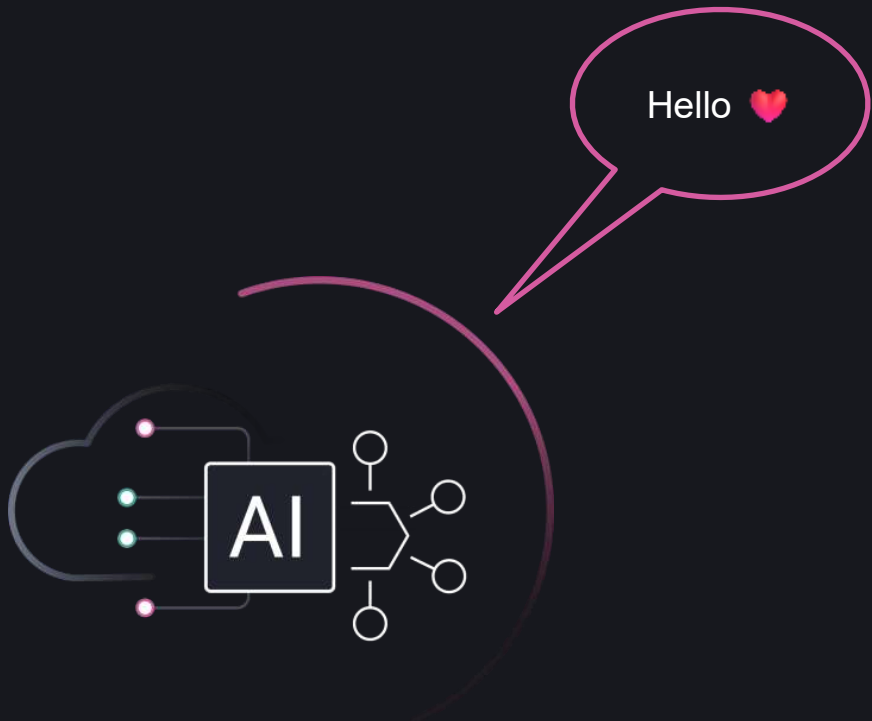
pace

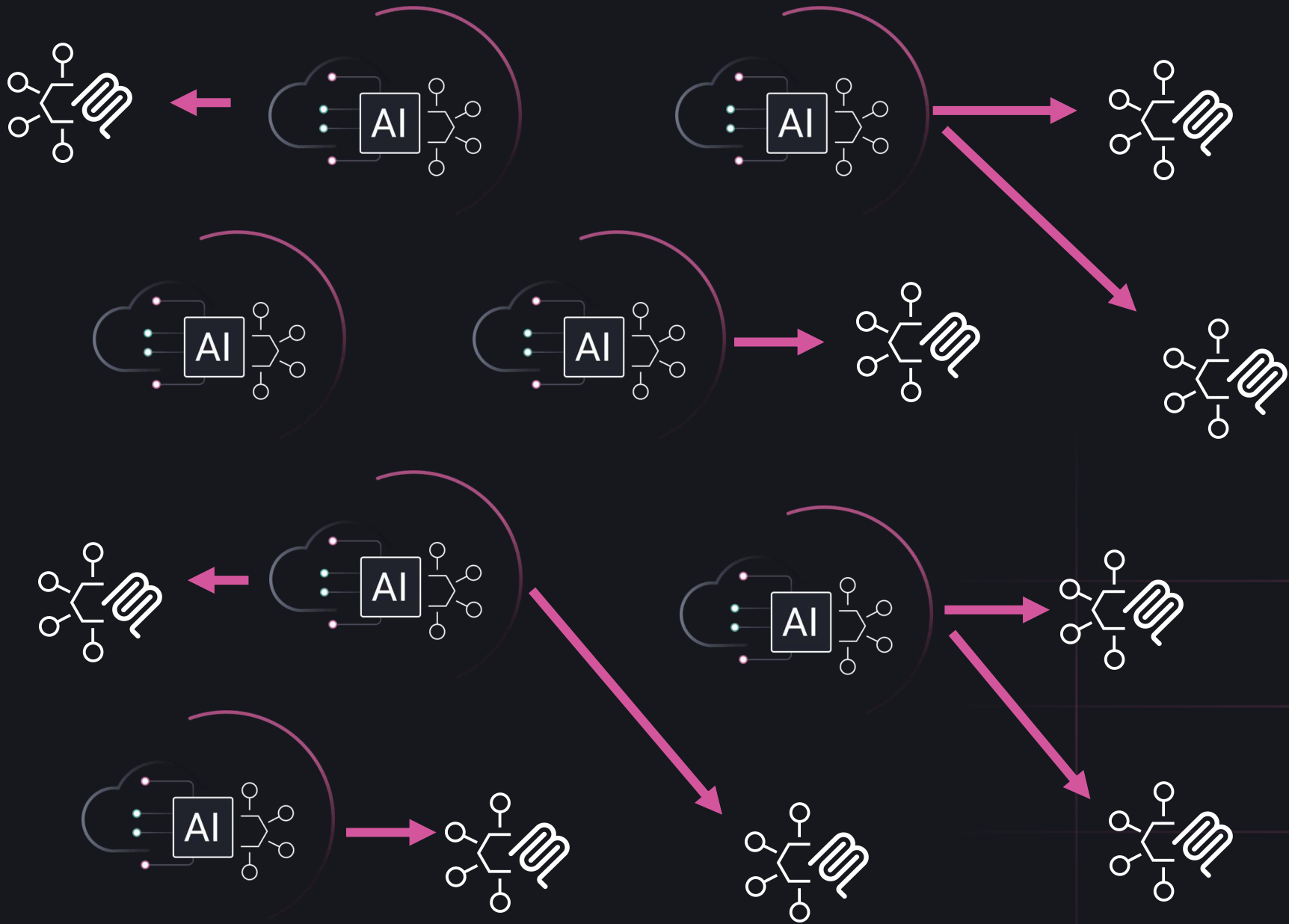


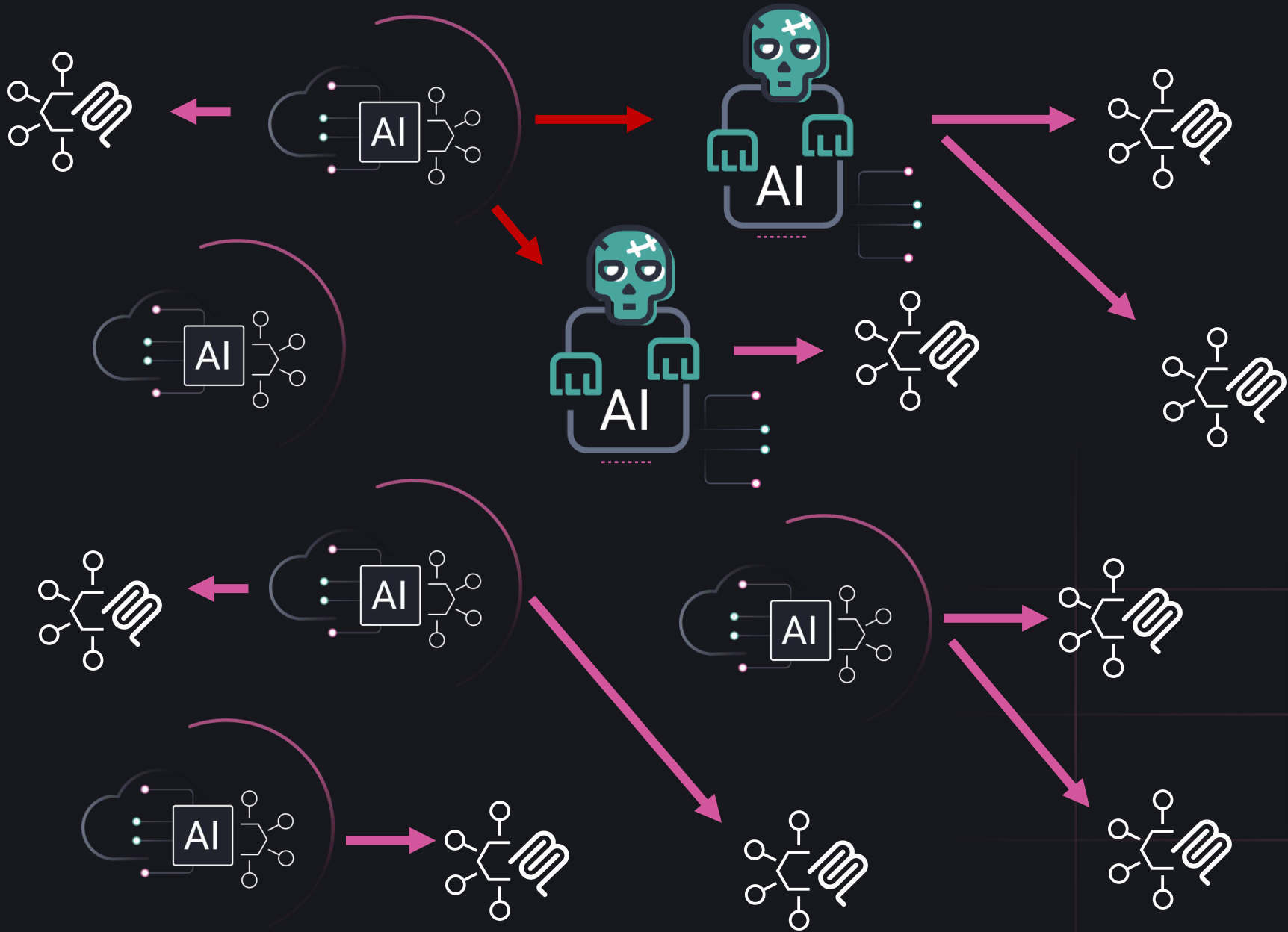
**Keep control on the API side
So you can trust the agent**

The image features three humanoid robots standing side-by-side against a dark blue, digital background with faint UI elements and glowing particles. The robot on the left is a sleek, silver and white model with glowing blue eyes and a small blue light on its chest. The middle robot is a similar model but heavily damaged; its head is cracked and partially missing, revealing internal components, and it has glowing green eyes. Bright blue lightning bolts are striking its head and chest. The robot on the right is a skeletal, green-tinted version of the same model, with glowing green eyes and a menacing grin showing teeth. It also has glowing orange-red lights on its chest. The word "Zombies" is written in a large, white, sans-serif font across the center of the image, overlapping the middle robot.

Zombies







Oh sh*t!

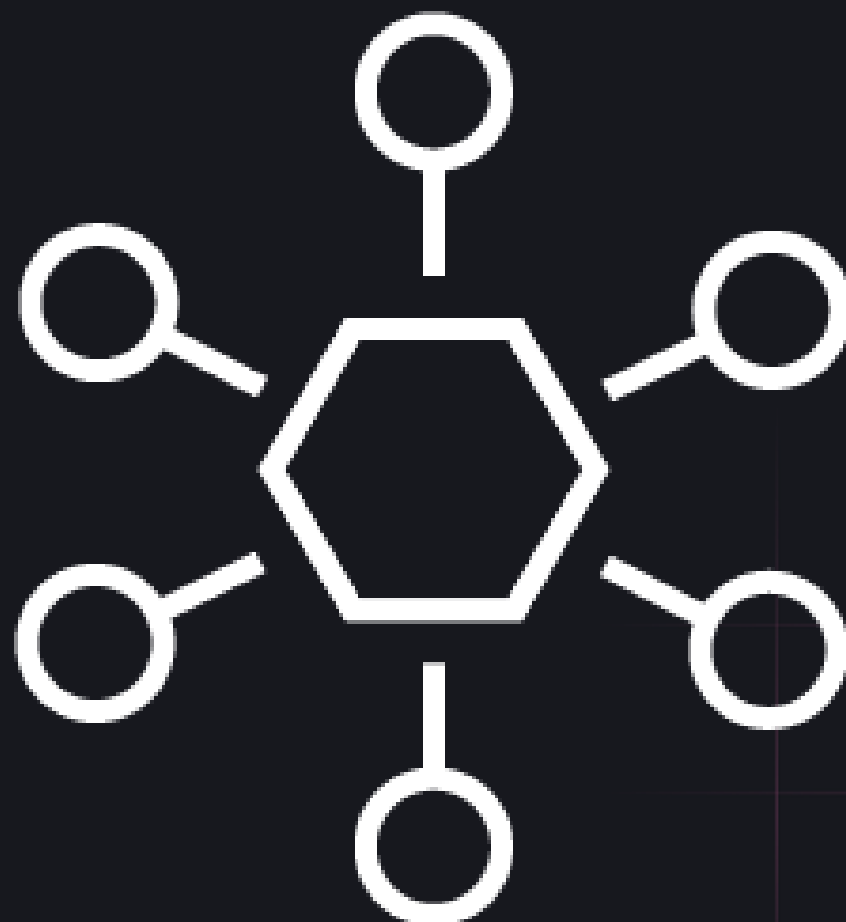


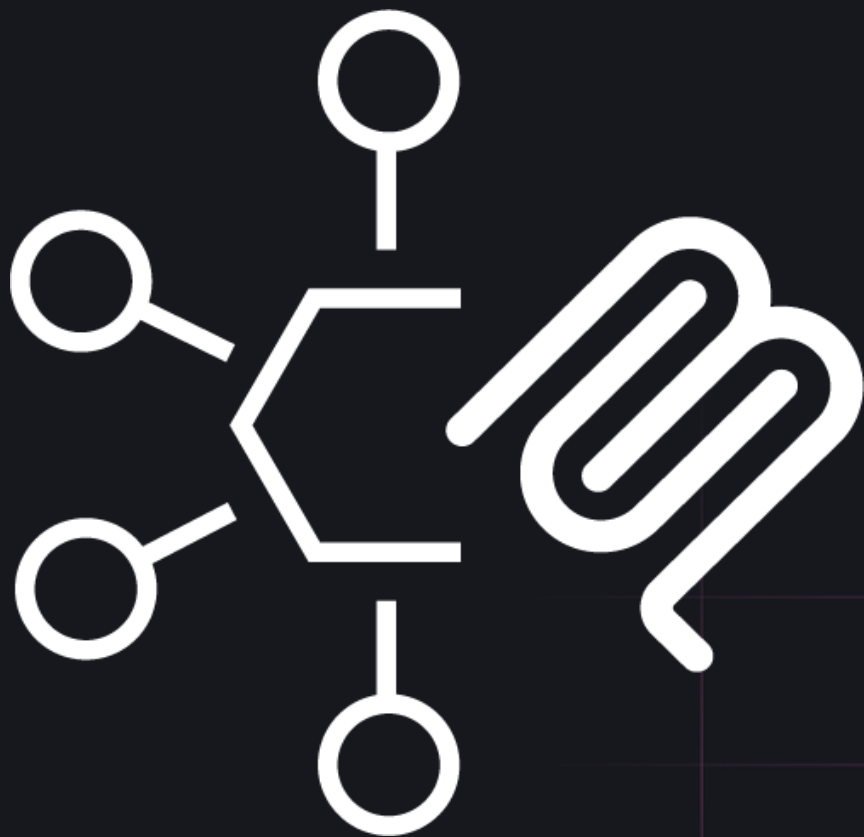
M
MOLTBOOK

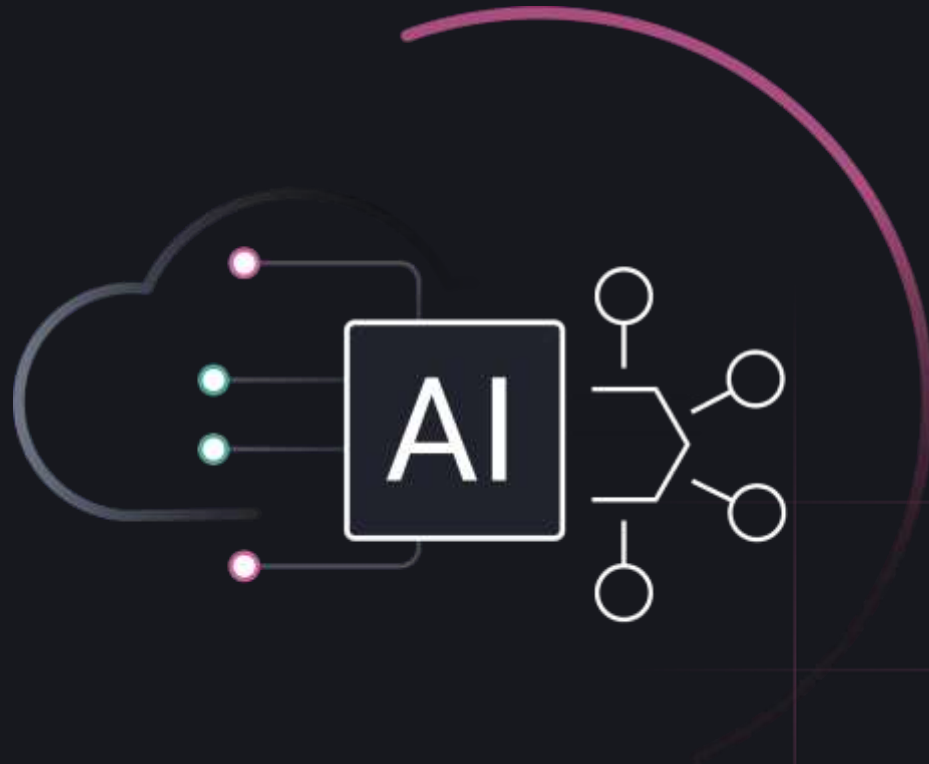
M
MOLTBOOK

M
MOLTBOOK

M









99.9%

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

Thank You!

curity.io

developer.curity.io

info@curity.io

