Trustworthy Identity and Access Control for Agentic AI

Marcelo Yannuzzi

Principal Engineer, Cisco

ITU Workshop on "Trustable and Interoperable Digital Identities for Human and Agentic AI”

Session 3: Challenges on authorization and delegation in the context of agentic AI

March 31st 2026, Geneva, Switzerland

It all starts with Identity ...

The Identity Zoo

cisco DUO

KEYCLOAK

okta

Microsoft Entra ID

ORY

PingIdentity.

3rd party IDs

Accounts @IdPs

SPIFFE / SPIRE

NHI

Well-known URLs

?

X.509 CERTs / new ones

Decentralized IDs (DIDs)

Agent Name Service (ANS)

OpenID Connect Agent IDs

Our Response

AGNTCY

THE LINUX FOUNDATION

An open-source project for inter-agent collaboration

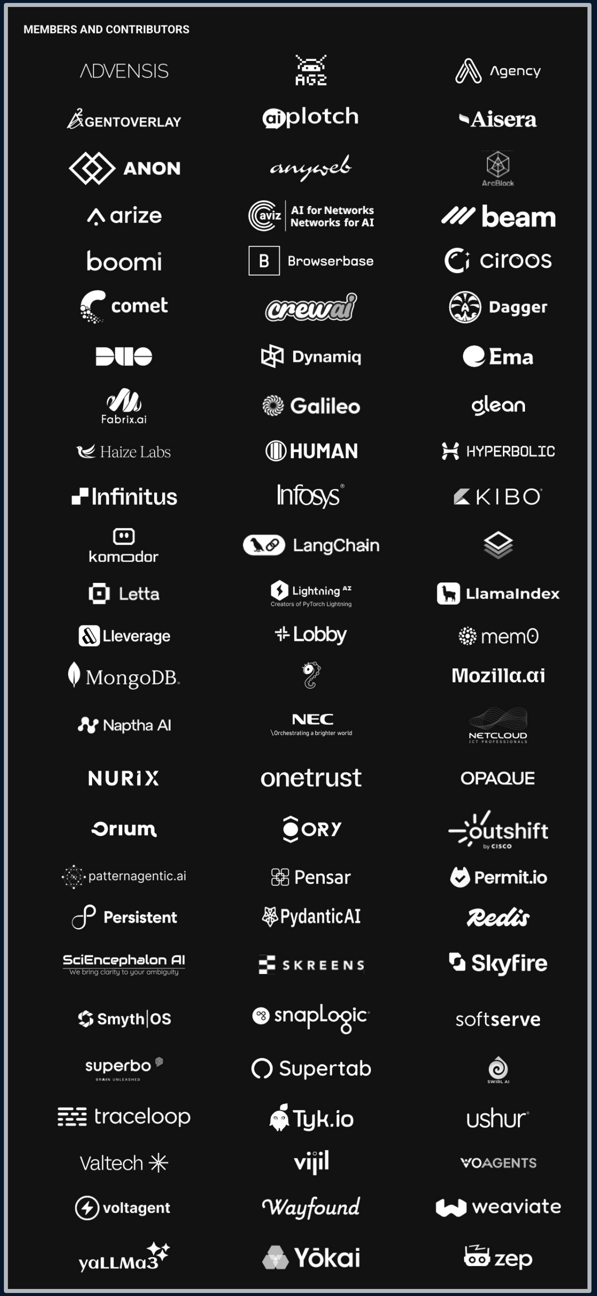
TECHNICAL STEERING COMMITTEE

CISCO Google DELL Red Hat ORACLE

80+ collaborating organizations

AGNTCY: https://agntcy.org

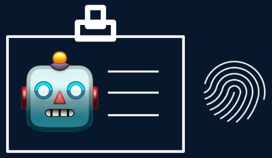
Identity Working Group: https://github.com/agntcy/governance/blob/main/working-groups/identity/CHARTER.md



MEMBERS AND CONTRIBUTORS

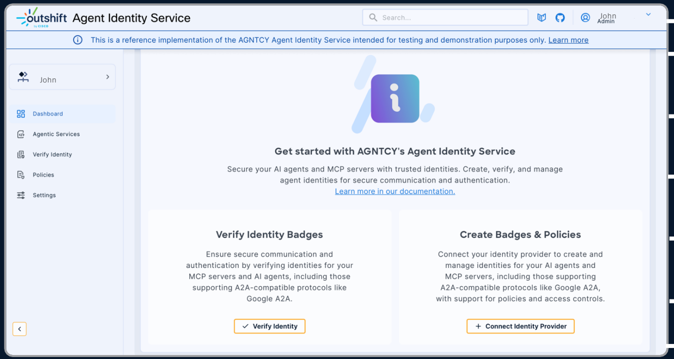
ADVENSIS
AG2
Agency
AGENTOVERLAY
aiplotch
Aisera
ANON
anyweb
ArcBlock
arize
aviz AI for Networks Networks for AI
beam
boomi
Browserbase
ciroos
comet
crewai
Dagger
DUO
Dynamiq
Ema
Fabrix.ai
Galileo
glean
Haize Labs
HUMAN
HYPERBOLIC
Infinitus
Infosys
KIBO
komodor
LangChain
Letta
Lightning AI Creators of PyTorch Lightning
LlamaIndex
Lleverage
Lobby
mem0
MongoDB
Mozilla.ai
Naptha AI
NEC \Orchestrating a brighter world
NETCLOUD ICT PROFESSIONALS
NURIX
onetrust
OPAQUE
Orium
ORY
outshift by cisco
patternagentic.ai
Pensar
Permit.io
Persistent
PydanticAI
Redis
SciEncephalon AI We bring clarity to your ambiguity
SKREENS
Skyfire
Smyth|OS
snapLogic
softserve
superbo BRAIN UNLEASHED
Supertab
SWIRL AI
traceloop
Tyk.io
ushur
Valtech
vijil
VOAGENTS
voltagent
Wayfound
weaviate
yaLLMa3
Yōkai
zep

Trusted Identities



IDENTITY BADGE

AGNTCY Reference Implementation



outshift Agent Identity Service

This is a reference implementation of the AGNTCY Agent Identity Service intended for testing and demonstration purposes only. Learn more

Get started with AGNTCY's Agent Identity Service

Secure your AI agents and MCP servers with trusted identities. Create, verify, and manage agent identities for secure communication and authentication.
Learn more in our documentation.

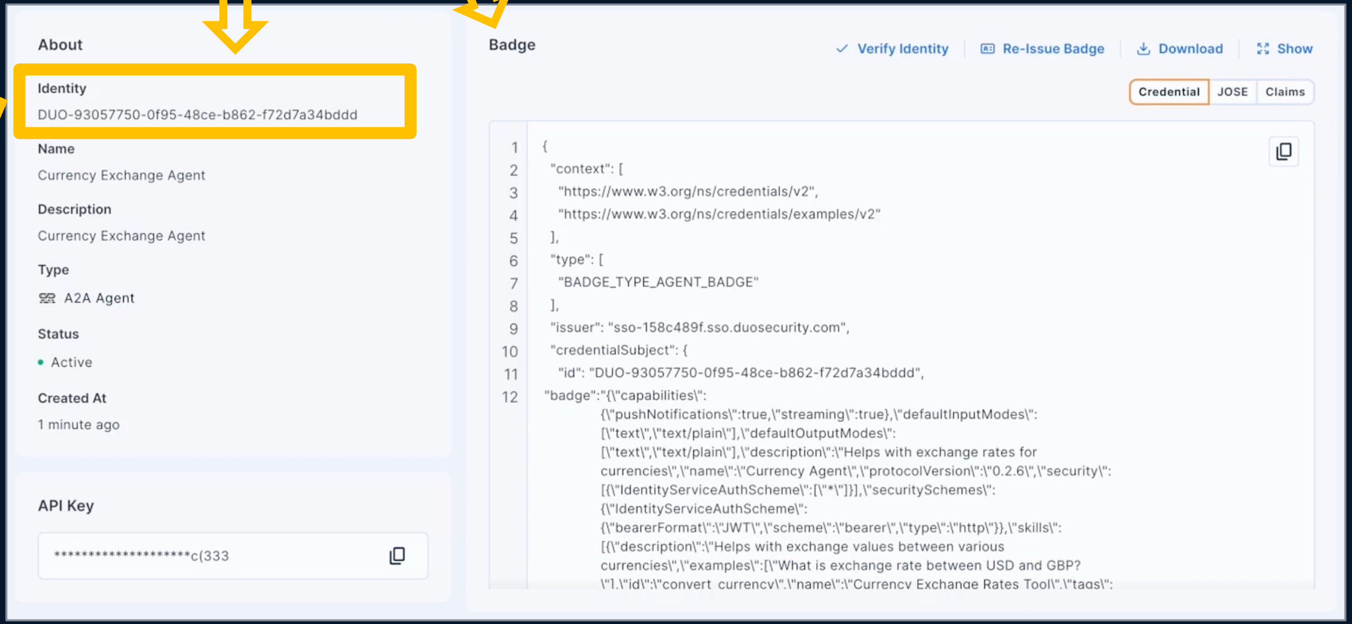
Verify Identity Badges

Ensure secure communication and authentication by verifying identities for your MCP servers and AI agents, including those supporting A2A-compatible protocols like Google A2A.

Create Badges & Policies

Connect your identity provider to create and manage identities for your AI agents and MCP servers, including those supporting A2A-compatible protocols like Google A2A, with support for policies and access controls.

- CISCO DUO
- okta
- ORY
- KEYCLOAK
- AGNTCY DIDs
- Microsoft Entra ID
- PingIdentity



About

Identity
DUO-93057750-0f95-48ce-b862-f72d7a34bddd

Name
Currency Exchange Agent

Description
Currency Exchange Agent

Type
A2A Agent

Status
● Active

Created At
1 minute ago

API Key
**********************c(333

Badge

```
{
  "context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "type": [
    "BADGE_TYPE_AGENT_BADGE"
  ],
  "issuer": "sso-158c489f.sso.duosecurity.com",
  "credentialSubject": {
    "id": "DUO-93057750-0f95-48ce-b862-f72d7a34bddd",
 "badge":"{\"capabilities\":
             {\"pushNotifications\":true,\"streaming\":true},\"defaultInputModes\":
             [\"text\",\"text/plain\"],\"defaultOutputModes\":
             [\"text\",\"text/plain\"],\"description\":\"Helps with exchange rates for
             currencies\",\"name\":\"Currency Agent\",\"protocolVersion\":\"0.2.6\",\"security\":
             [{\"IdentityServiceAuthScheme\":[\"*\"]}],\"securitySchemes\":
             {\"IdentityServiceAuthScheme\":
             {\"bearerFormat\":\"JWT\",\"scheme\":\"bearer\",\"type\":\"http\"}},\"skills\":
             [{\"description\":\"Helps with exchange values between various
             currencies\",\"examples\":[\"What is exchange rate between USD and GBP?
             \"],\"id\":\"convert_currency\",\"name\":\"Currency Exchange Rates Tool\",\"tags\":
```

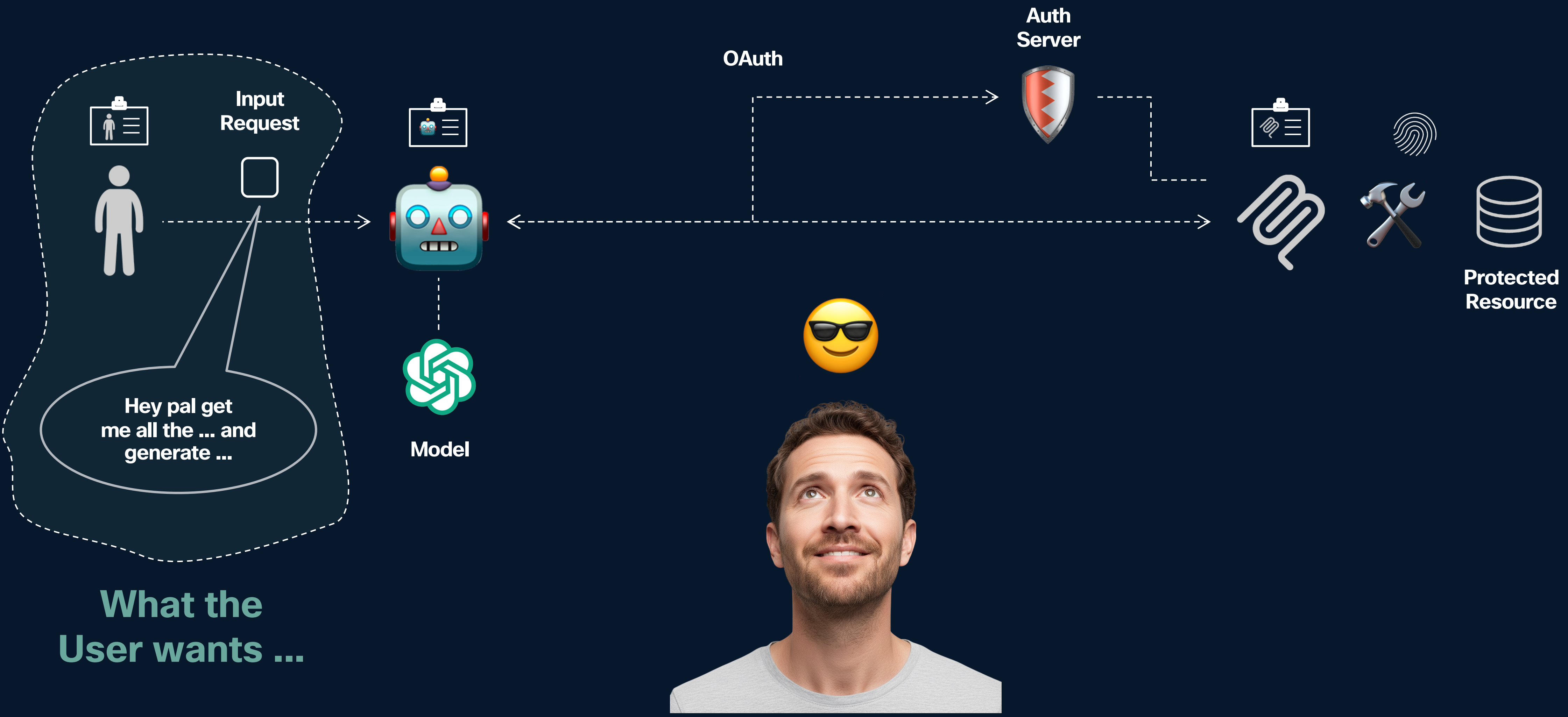
SaaS: https://agent-identity.outshift.com/welcome

OSS: https://github.com/agntcy/identity-service

Demo: https://www.youtube.com/watch?v=CO3YwjRXyOo

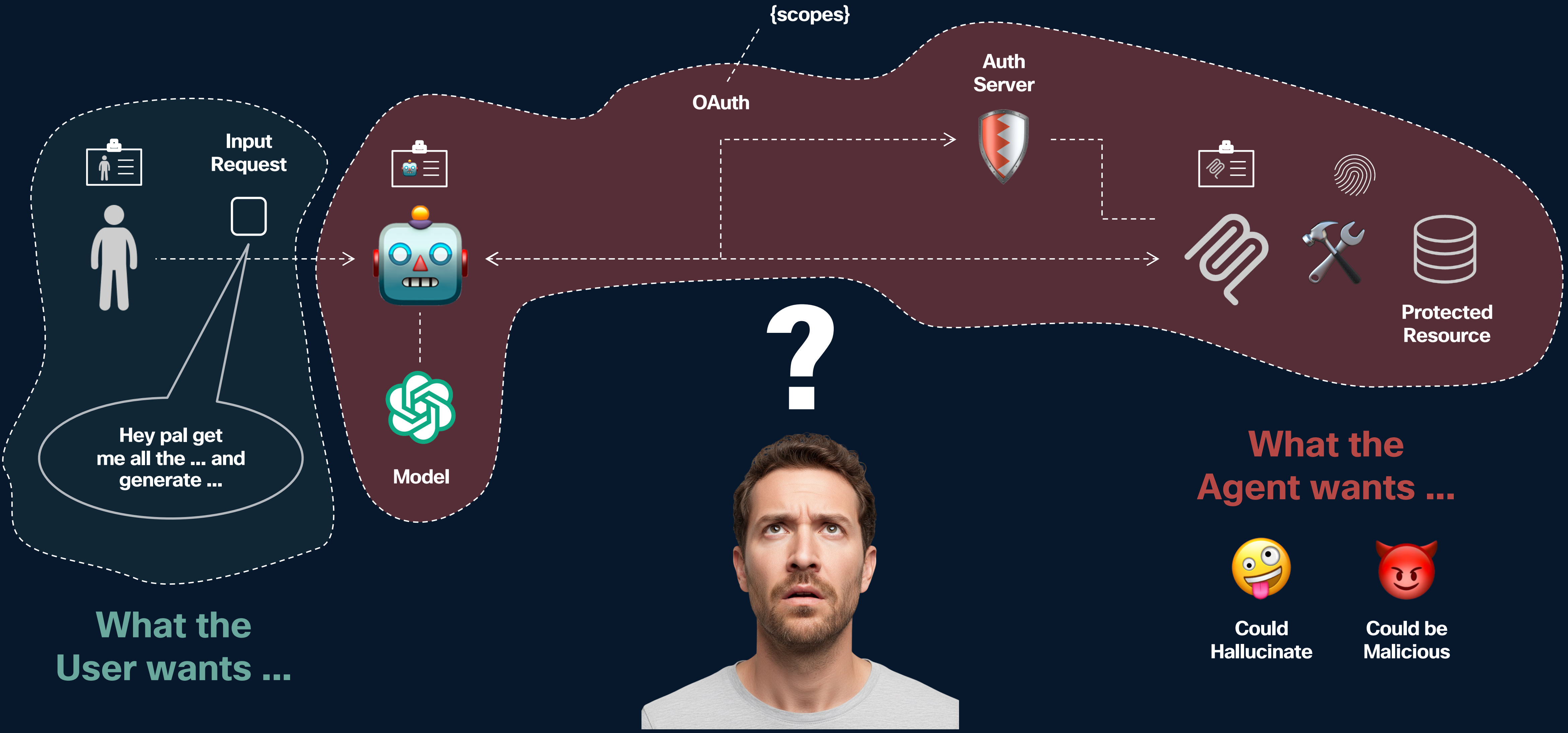
Controlling the Agents’ Actions

Doesn’t sound that complex ...



What the
User wants ...

... but wait a minute ...



What the User wants ...

What the Agent wants ...

🤪 Could Hallucinate

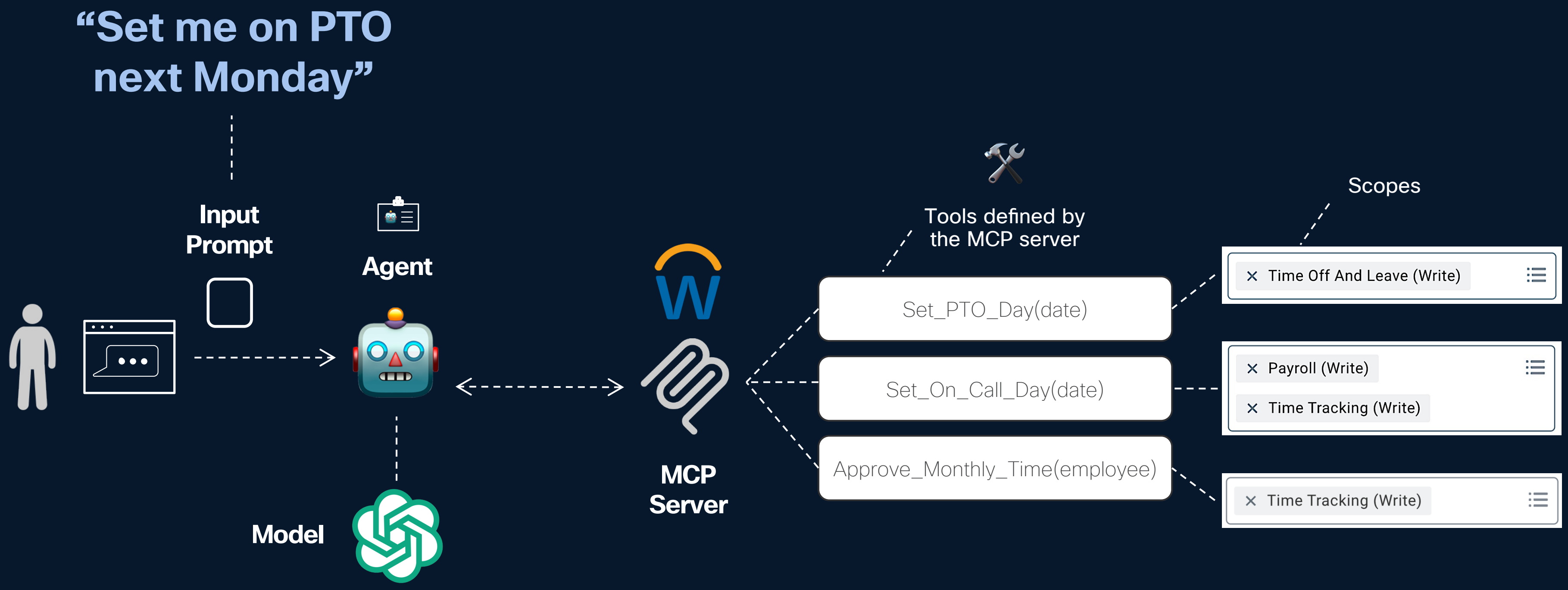
😈 Could be Malicious

Access Control in the Era of Agentic AI ...

Do we trust their intentions?

Bridging the disconnect in Access Control

Task-Based Access Control (TBAC)



“Set me on PTO next Monday”

Input Prompt

Agent

Model

MCP Server

Tools defined by the MCP server

Set_PTO_Day(date)

Set_On_Call_Day(date)

Approve_Monthly_Time(employee)

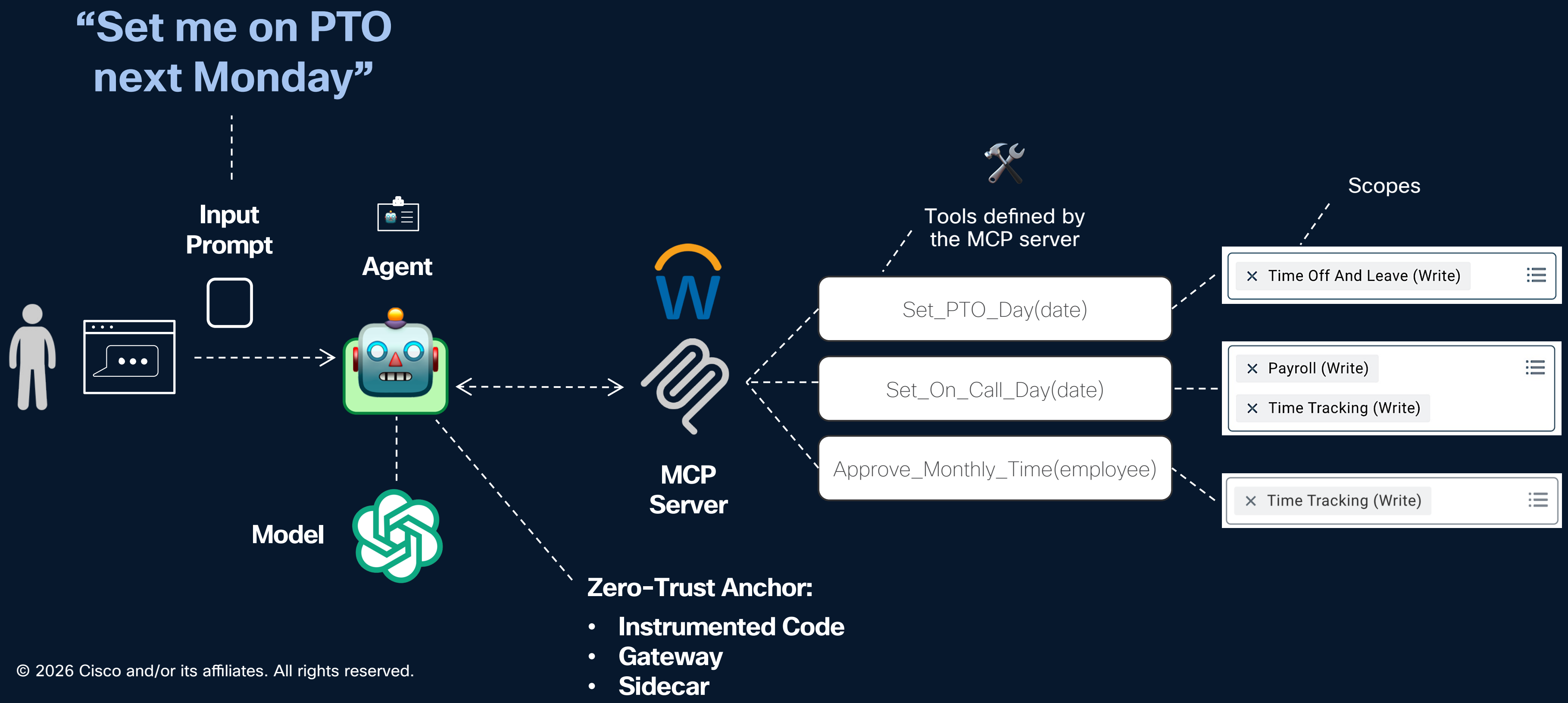
Scopes

× Time Off And Leave (Write)

× Payroll (Write)
× Time Tracking (Write)

× Time Tracking (Write)

Task-Based Access Control (TBAC)



“Set me on PTO next Monday”

Input Prompt

Agent

Model

MCP Server

Tools defined by the MCP server

Set_PTO_Day(date)

Set_On_Call_Day(date)

Approve_Monthly_Time(employee)

Scopes

× Time Off And Leave (Write)

× Payroll (Write)

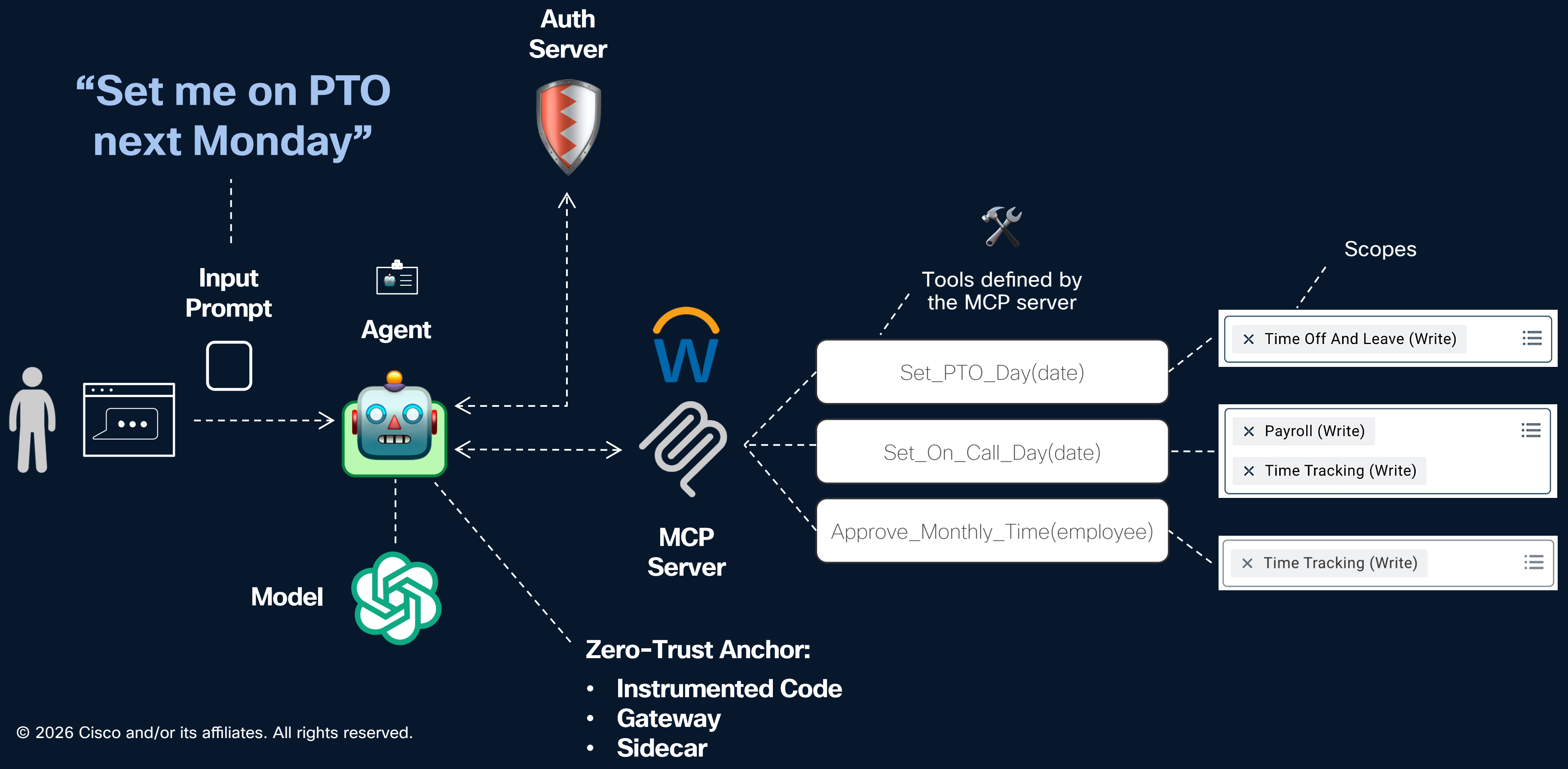
× Time Tracking (Write)

× Time Tracking (Write)

Zero-Trust Anchor:

- Instrumented Code
- Gateway
- Sidecar

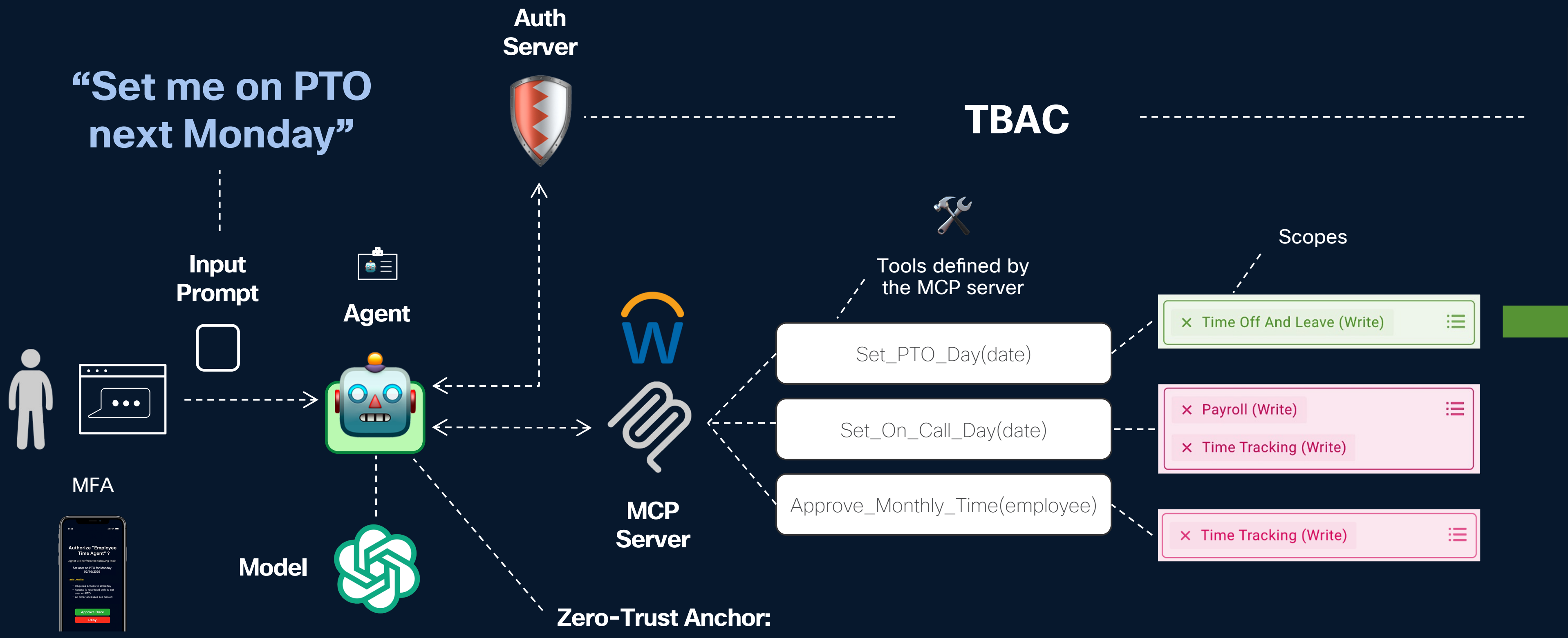
Task-Based Access Control (TBAC)

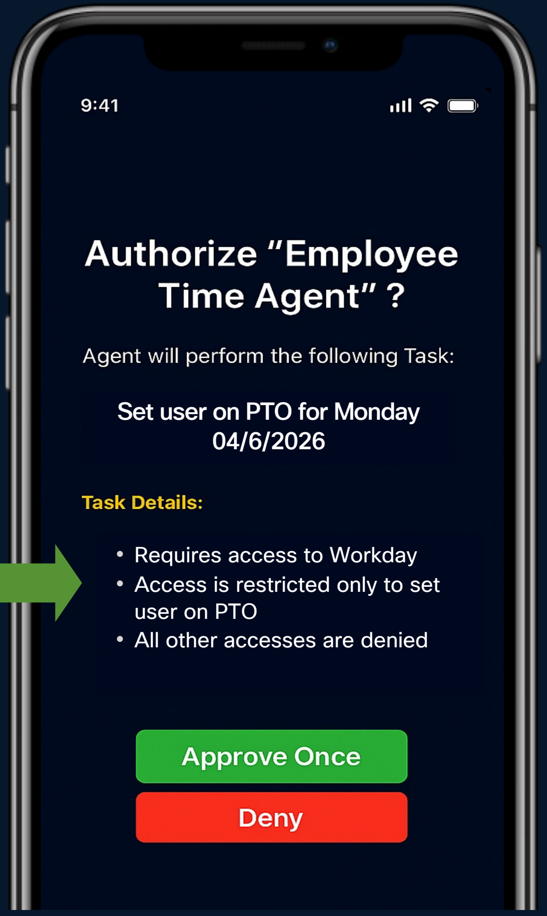


Zero-Trust Anchor:

- **Instrumented Code**
- **Gateway**
- **Sidecar**

Task-Based Access Control (TBAC)





9:41

Authorize "Employee Time Agent" ?

Agent will perform the following Task:

Set user on PTO for Monday 04/6/2026

Task Details:

- Requires access to Workday
- Access is restricted only to set user on PTO
- All other accesses are denied

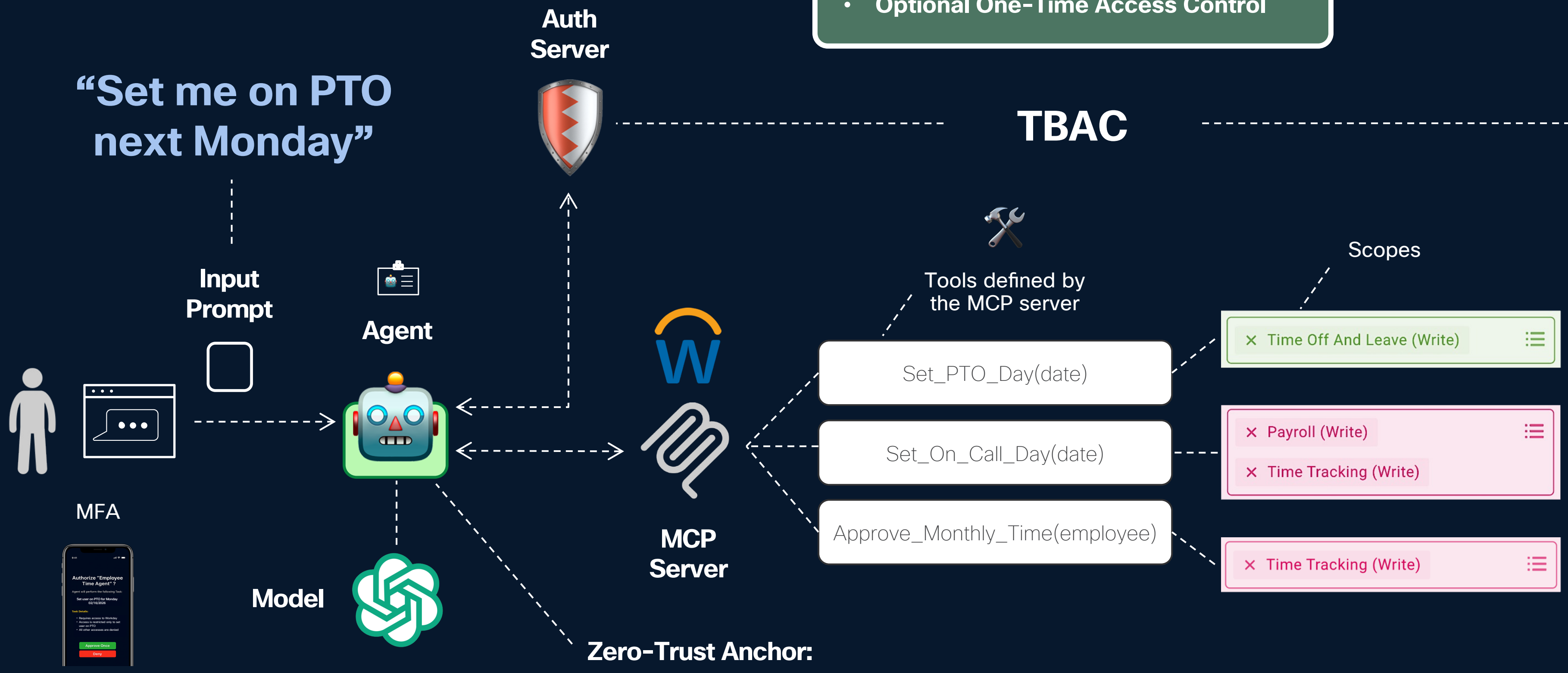
Zero-Trust Anchor:

- **Instrumented Code**
- **Gateway**
- **Sidecar**

Task-Based Access Control (TBAC)

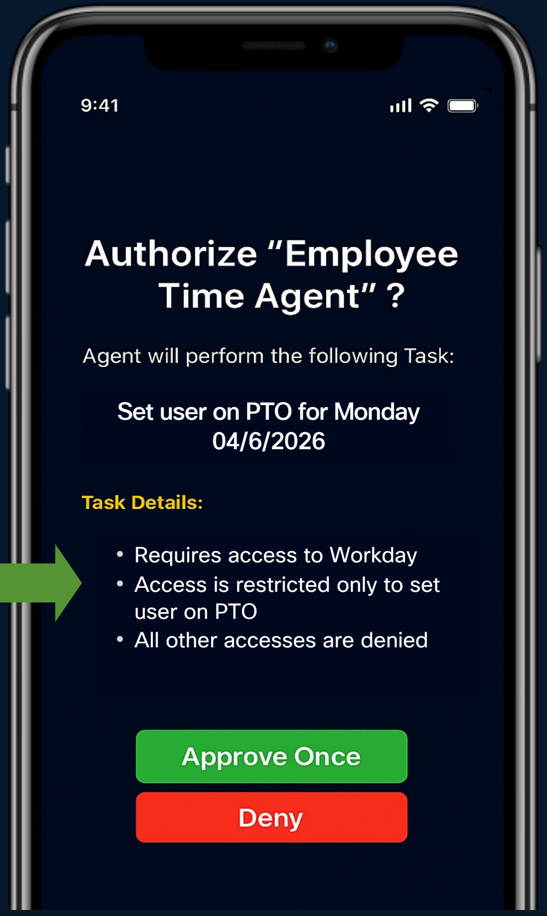
With TBAC

- Full visibility into the specific task
- Only necessary scopes are approved
- Scopes and tools tied to the task
- Optional One-Time Access Control



Zero-Trust Anchor:

- Instrumented Code
- Gateway
- Sidecar



Authorize "Employee Time Agent" ?

Agent will perform the following Task:

Set user on PTO for Monday 04/6/2026

Task Details:

- Requires access to Workday
- Access is restricted only to set user on PTO
- All other accesses are denied

Call to action

AGNTCY website

https://agntcy.org/

AGNTCY Agent Identity Service

https://github.com/agntcy/identity-service/

AGNTCY Agent Identity GitHub repository

https://github.com/agntcy/identity

Thank You!

cisco