



Agentic AI Foundation

AGNTCon + MCPCon

North America

Where the **agentic stack** is being built.

Building the Internet of Agents in the Open

Mazin Gilbert, Executive Director, AAIF

Agentic AI Foundation Vision & Strategy



INTEROPERABILITY

Enable the Internet of Agents

Open protocols let any agent work with any tool and any other agent, without a custom integration for each pair.



OPEN STACK

Define the agentic stack in the open

We develop the stack under neutral governance, so no single company controls it and anyone can inspect and improve it.



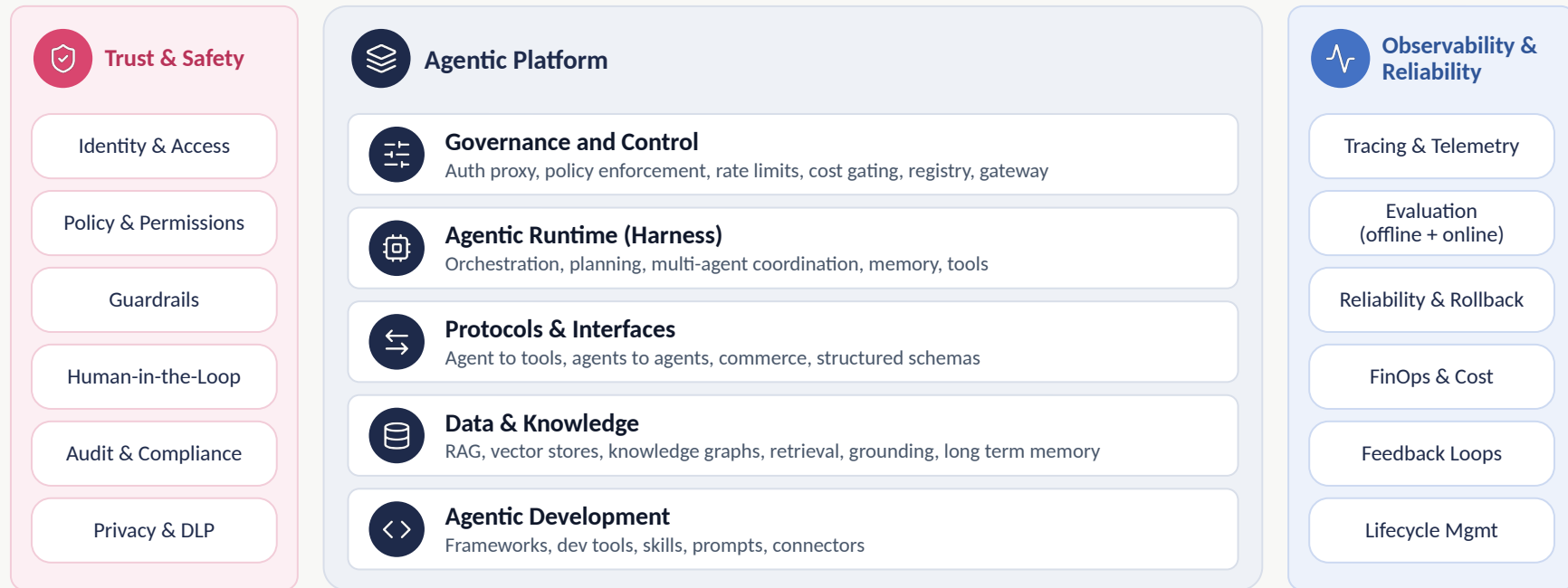
GLOBAL COMMUNITY

Grow a global community

Members, end users, and developers in every region work together to put open standards into production.

Open source and open standards are the foundations that enable Agentic AI to scale safely

Agentic AI Stack Defined



Same model. Different harness. Different agent. *We standardize the seams, not the internals.*

AAIF Projects

AAIF is host to top open source technology projects in agentic AI.

Model Context Protocol

Model Context Protocol (MCP) is a protocol for seamless integration between LLM applications and external data sources.

goose

An open source, extensible AI agent that goes beyond code suggestions. Install, execute, edit, and test with any LLM.

AGENTS.md

AGENTS.md is a simple, open format for guiding coding agents.

agentgateway

agentgateway enables secure, scalable connections between AI agents, models, tools, and APIs across ecosystems.

Agent2Agent (A2A)

An open protocol that lets AI agents communicate, collaborate, and exchange tasks across platforms.

Agent Router

An open source AI gateway, built on Envoy, that connects applications to models and MCP tools.

OpenSandbox

A secure sandbox platform for running agent code and tools in isolation, with a unified API and SDKs.

Open Responses

An open specification for interoperable LLM interfaces, so agents can call models from many providers the same way.

Agent Skills

Agent Skills is an open format for giving agents new capabilities, knowledge, and workflows.

OpenEnv

An open framework and hub for agent environments, used to train and evaluate agents with reinforcement learning.

Working Groups and Committees

WORKING GROUPS *Member-led and open to anyone. Meetings, mailing lists and repos are public.*

01 Accuracy & Reliability
Accuracy collapses over long, multi-step task chains.

02 Agentic Commerce
Converging ACP, UCP, x402 and AP2 for agent payments.

03 Governance, Risk & Regulatory
Accountability for agent errors, across jurisdictions.

04 Identity & Trust
Who an agent is, who it acts for, and what it may do.

05 Observability & Traceability
Audit trails across tools, sub-agents, and long runs.

06 Security & Privacy
Stopping prompt injection and tool poisoning attacks.

07 Workflows & Process Integration
Orchestration and human review patterns across vendors.

08 Taxonomy & Landscape
Shared glossary of agentic AI terms and ecosystem map.

BOARD COMMITTEES

Government Affairs

Works with governments and regulators on agentic AI policy and public sector adoption.

ANDxOR End Users

Enterprise end users working together to adopt agentic AI at scale, within and across companies.

Applied Industries

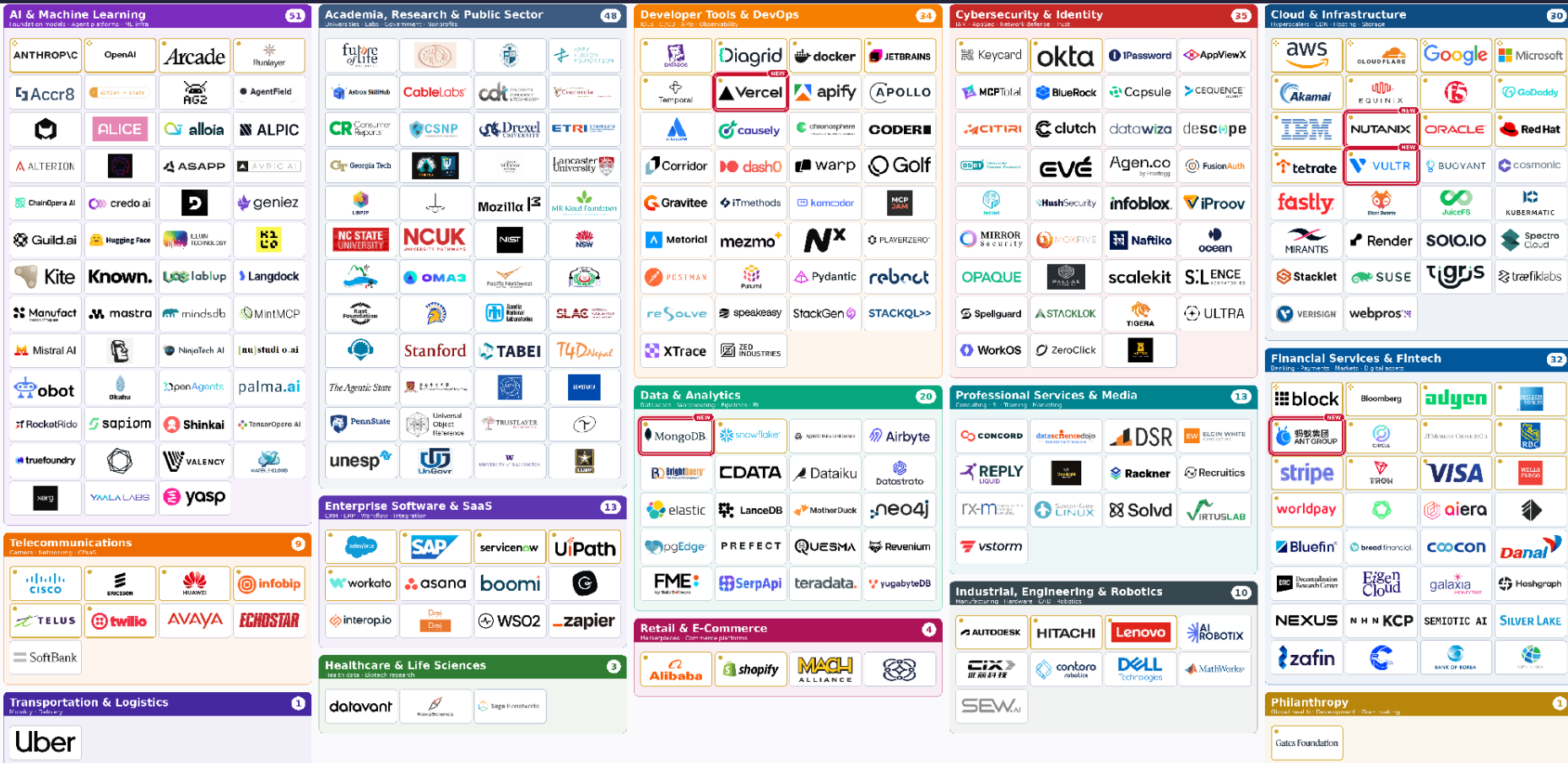
Defines common requirements for regulated industries and feeds findings to working groups and standards bodies.

Startups

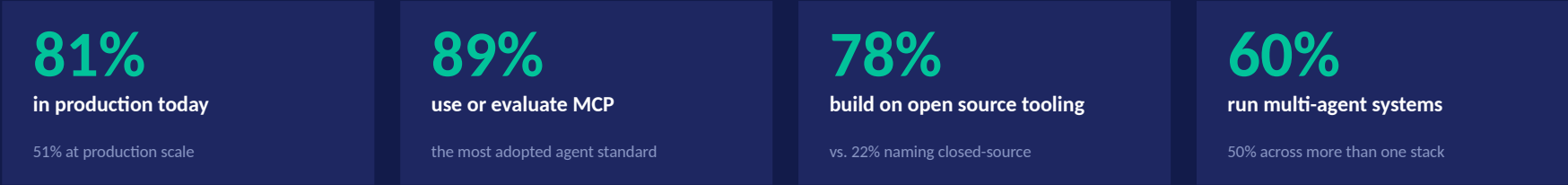
Startups meet regularly to share learnings, network, and give startups a stronger voice in AAIF.

AAIF Member Landscape

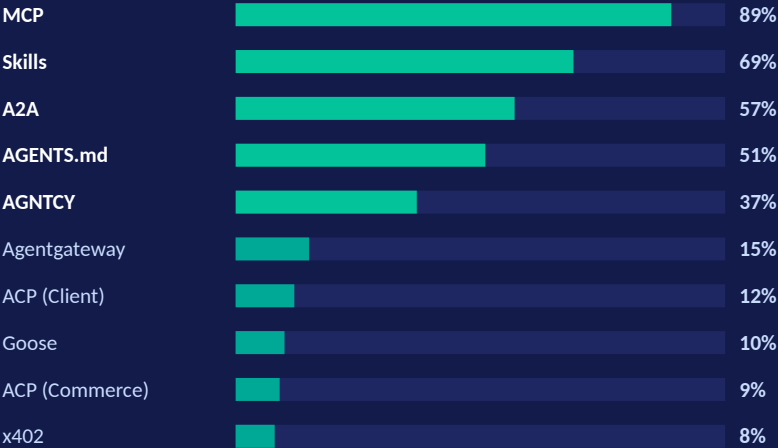
305 Members across 15 industrial sectors



Agentic AI Is Already a Production Market



THE OPEN STANDARDS STACK — TOP 10 ADOPTED



Using or actively evaluating (select all that apply, n=175). MPP follows at 6%.

OPEN SOURCE DOMINATES THE TOOLING LAYER



Share naming at least one tool of each type. Unaided open text (n=185), so the groups overlap.

Most-named open source

LangGraph · LangChain · AGNTCY · Google
ADK · MCP · CrewAI

Most-named closed source

Anthropic ecosystem · Cursor · Codex ·
Gemini

OVERSIGHT IS A DESIGN CHOICE

66% human-on-the-loop · 63% bounded autonomy · 23% fully autonomous

DEPLOYMENT IS HYBRID BY DEFAULT

85% public cloud · 56% on-prem · 42% local/desktop · 19% edge

The Future is Agentic. Let's Build It Together.

Six ways to start this week — scan any code.



AAIF

Who we are, our members,
and how to join.

aaif.io



Newsletter

Weekly updates on agentic
AI standards.

aaif.io/#subscribe-modal



Working Groups

All eight. Meetings and
repos are public.

aaif.io/working-groups



Submit a Project

Bring your project to a
neutral home.

aaif.io/submit-a-project



Events

AGNTCon, MCPCon,
AGNT Summits, and local
meetups.

aaif.io/events



Contribute to AAIF Projects

All ten projects, from MCP
to OpenEnv.

github.com/aaif

Contribute code, technical architecture, reference implementation, designs, or industry knowledge

Agentic AI Foundation



AGNTCon + MCPCon

North America

Where the **agentic stack** is being built.