OUTSELL PLAYBOOK

OUTSELL JOURNAL - DECISION WORKSHEET

Agent runtime identity: an evidence plan from authority to action

QUESTION

How should enterprise AI vendors and services teams prove that an agent's identity, delegated authority and runtime actions remain controlled?

GUIDE TAKEAWAY

Registration and login are only the start. Bind each agent to an owner and purpose, constrain delegated authority, issue short-lived access, observe actual use and test revocation with evidence that a buying group can inspect.

START HERE

Register the agent, owner, purpose and version.

YOUR SITUATION

Account or cohort

Decision to make

Starting state and exclusions

Evidence sources, dates, and limitations

Unknowns to validate

WORK THROUGH THE GUIDE

1. Register the agent, owner, purpose and version

Evidence or input

Output or decision

Owner and review point

2. Define delegation ceiling and credential lifetime

Evidence or input

Output or decision

Owner and review point

3. Correlate identity, tool and resource activity

Evidence or input

Output or decision

Owner and review point

4. Rehearse denial, expiry and emergency revocation

Evidence or input

Output or decision

Owner and review point

5. Publish dated evidence and unresolved gaps by buyer role

Evidence or input

Output or decision

Owner and review point

COMPARE THE OPTIONS

Static service credential

Useful when: A deterministic workload has fixed permissions

Limitation: Long life can widen exposure

Suggested action: Rotate and bind to a narrow service

Why this fits our situation

Evidence needed before acting

Registered agent identity

Useful when: Agent versions need ownership and policy

Limitation: Registration alone does not govern behavior

Suggested action: Link each run to owner and purpose

Why this fits our situation

Evidence needed before acting

On-behalf-of delegation

Useful when: A user authorises a bounded task

Limitation: Scope can drift across tools

Suggested action: Enforce ceilings and short expiry

Why this fits our situation

Evidence needed before acting

Human-approved execution

Useful when: Consequence requires accountable judgment

Limitation: Review can become ceremonial

Suggested action: Show evidence and retain stop authority

Why this fits our situation

Evidence needed before acting

COMMIT TO A BOUNDED NEXT STEP

Chosen action

Responsible owner

Required approval

Success measure and definition

Review date

Continue, revise, or stop criteria

Guide: https://outselll.com/blogs/agent-runtime-identity-evidence-plan/

Publisher and evidence policy: https://outselll.com/editorial-policy/