CLOUDBOLT

AI Agent Governance – Five Questions to Ask

Use these five questions to check whether each AI agent touching your infrastructure has access someone deliberately granted (provisioned) or access it picked up along the way (emergent). Each one comes with what a good answer looks like and a quick test to confirm it.

The five questions

If the answer to any of these is "I don't know," that agent has emergent access.

1

Who is it acting for?

GOOD ANSWER

A named user in your identity provider. The agent signs in as that user through the same SSO as any other app. No shared bot account, no key pasted into a config file.

HOW TO CHECK

Trace the agent's token back to a user. Disable that user and confirm the agent's next call fails.

2

What can it reach?

GOOD ANSWER

Exactly that user's groups and environments, on-prem and cloud, and nothing broader. Cloud and hypervisor credentials stay in the control plane; the agent never holds a key.

HOW TO CHECK

Ask the agent for something outside the user's group. Expect a denial, and expect it on the record.

3

What needs a human?

GOOD ANSWER

Reads by default. Writes only when the client asks for write scope. Well-known patterns run unattended and still get audited; production and destructive actions wait for a different person's approval.

HOW TO CHECK

Find who flags an action as needing approval, what the default is, and whether a requester can approve their own request.

4

Where is the record?

GOOD ANSWER

A request log line, an order, a job, and a resource history entry, all naming the same user and joined by ids, so one action can be followed end to end.

HOW TO CHECK

Pick one agent action and walk all four records. If it takes longer than a minute, or ends in a chat thread, the trail is not real.

5

How do I turn it off?

GOOD ANSWER

Disable the user in the identity provider and every agent session they opened ends with them. A single client's registration can be revoked on its own.

HOW TO CHECK

Do it once in a test environment and time it. The answer should be seconds, not a ticket.

Five moves for when the work leaves

The clouds and your integration tools are starting to run the work with their own agents, behind a boundary you cannot see through. Three things break when that happens. These five moves pay off whether the one-request build reaches you next quarter or next year.

What breaks

01

Completion is no longer yours to see

Did every agent finish? Did one invent a step? You get a report, not a view.

02

Attribution moves out of reach

The calls carry the role they ran under, not the order that asked. Agents that spawn agents compound it.

03

Every endpoint does it differently

AWS, Azure, Google, VMware, Proxmox and your integration tools each ship their own agents, logs and identities.

What to do now

1

Templates are the contract

WHAT IT MEANS

Clean, parameterized, in git. Whatever runs the build, yours or a vendor's agent, should only resolve to these.

HOW TO START

Take the three services you provision most and make each one a template an agent can fill in but not rewrite.

2

Policy before execution

WHAT IT MEANS

Entitlements, quota and approvals decided against the whole request, up front, instead of call by call.

HOW TO START

List every check that fires per API call today. Ask which ones still fire when seven hundred calls arrive as one request.

3

A plan you can approve

WHAT IT MEANS

For anything beyond a disposable environment, see what it intends before it does it. Known patterns run unattended; your chosen stops still stop.

HOW TO START

Require a readable plan for production and destructive requests. Let disposable environments run without one.

4

One system of record

WHAT IT MEANS

A request id that travels with the work, through every agent it spawns, and one place the evidence comes back to.

HOW TO START

Issue the id at your control plane. Once a month, pick one request and walk it from the order to the endpoint's own log and back.

5

Watch the endpoints

WHAT IT MEANS

When a cloud describes a tool as an outcome ("provision an environment") instead of an API call ("create a bucket"), the shift has arrived there.

HOW TO START

Read the release notes for AWS MCP Server, Amazon Bedrock AgentCore, Microsoft Foundry, Google Agent Runtime and the Terraform MCP server each quarter.

Get CloudBolt CMP free

CloudBolt CMP is free for up to 100 resources, MCP server included. Connect an agent and run it through the five questions. It signs in as a named user, works within that user's groups and approvals, and logs every action under that user. No credit card required.

Get started free →