CLOUD STRATEGY

Your Identity Provider Was Never Your Spend Boundary

Spend authority is assumed to inherit safely from identity authority. A single compromised account proves it doesn't.

Cloud Governance Treats These As Different Events

IDENTITY COMPROMISE

Security team.

IR playbook.

Credential rotation.

FINANCIAL COMPROMISE

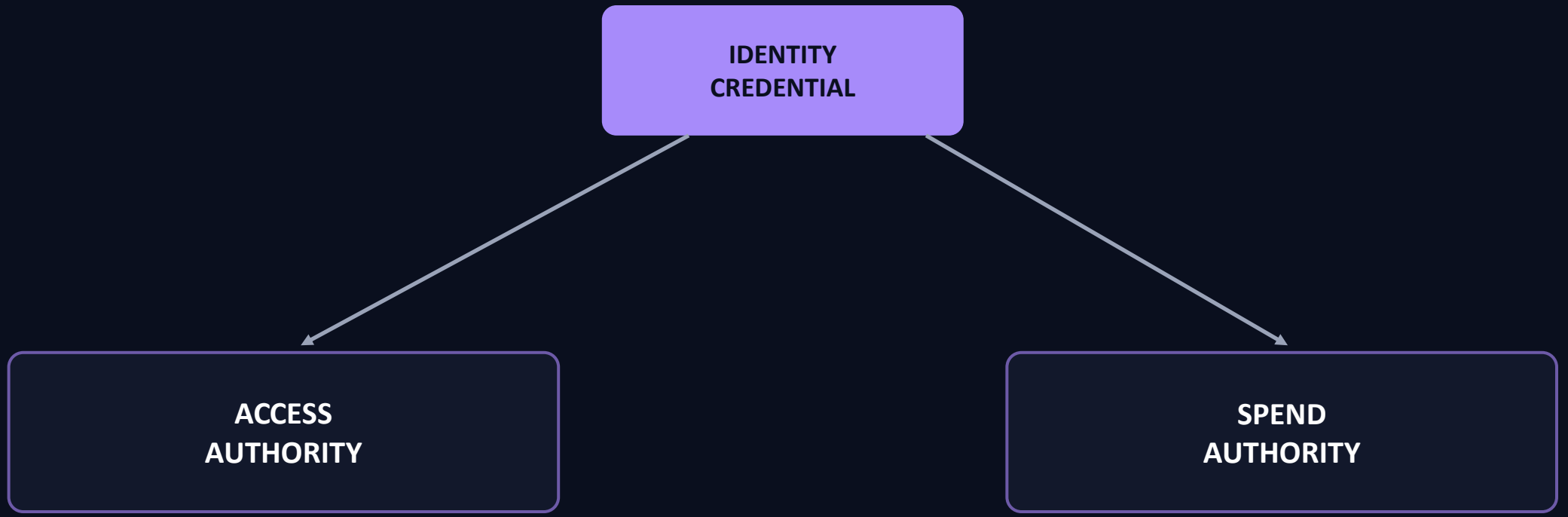
FinOps team.

Budget alert.

Cost anomaly review.

Two teams. Two playbooks. One actual event.

Same Authority Chain, Both Events



No second gate exists between “whether” and “how much.”

Run The Containment Test

Can it stop spend before authorization occurs?

Control	Stops spend before authorization?
Budget	No
Forecast	No
Alert	No
Dashboard	No
Hard policy enforcement	Sometimes

THE DIAGNOSTIC

“If an attacker obtained the credentials of your most privileged cloud privileged cloud operator, what mechanism would stop them from from authorizing six figures of new spend before a human intervened?” intervened?”

Spend Authority Isn't Separate — It's Inherited

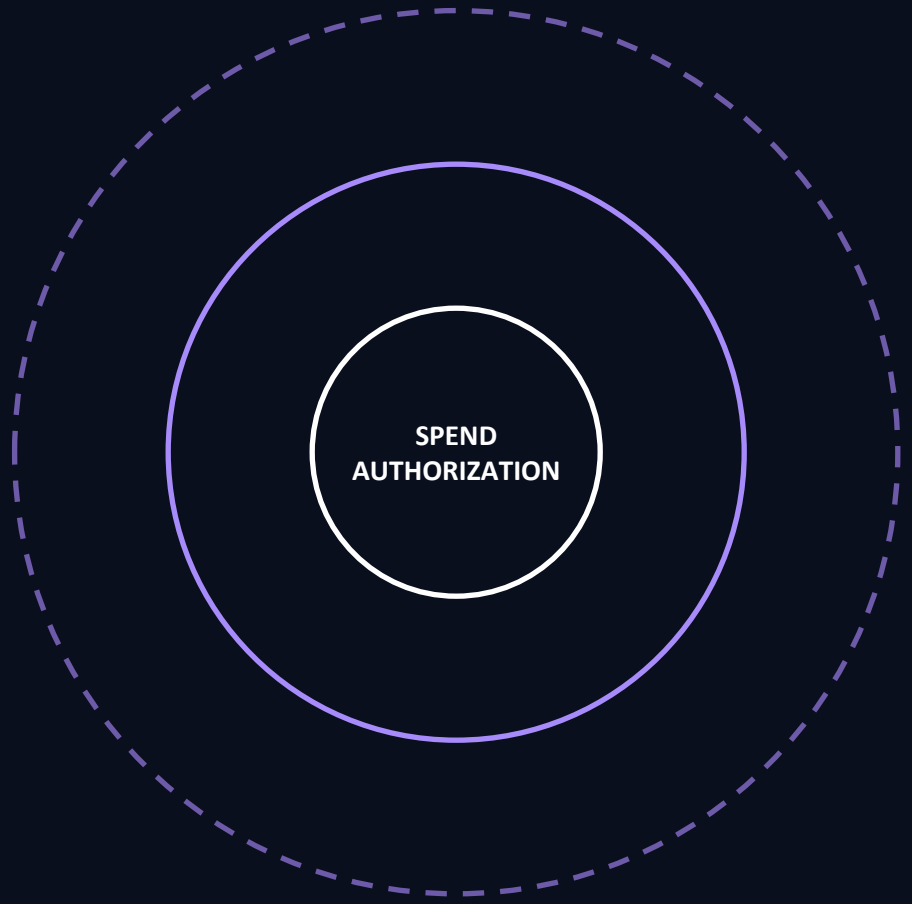
WHO CAN ACT

Roles, conditional access, JIT elevation, session risk scoring — mature and well-governed.

HOW MUCH THEY CAN SPEND

No independent ceiling. No separate review. Inherited silently from the first answer.

This Is Identity Boundary Inversion, Applied To Money



Framework #160: identity — not network topology — determines whether an action is authorized and survivable.

Spend authorization is no exception.

What An Actual Spend Boundary Requires

1. Enforcement that doesn't derive its authority from the identity chain it's meant to check
2. A ceiling that holds regardless of which credential is presenting the request
3. Spend authority reviewed as its own governance question — not assumed from access authority

A Boundary Untested Under Compromise Was Never A Boundary.

It was a convenience that hadn't been tested yet.

rack2cloud.com | Follow The Architect for more