Email **Off**
Access **On**

EMAIL DISABLED

ACCESS REMAINS OPEN

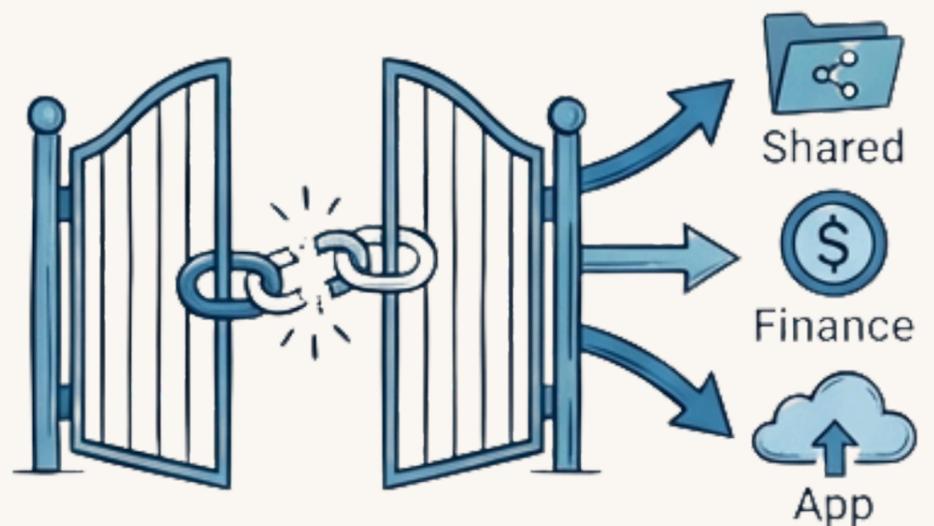*Wylie Blanchard*

Offboarding has 3 layers

1. IDENTITY
(who you are)

HR & SSO often disable the main account

2. ACCESS
(what you can do)

Permissions often remain active

3. DATA
(what you can still reach)

Data paths stay open
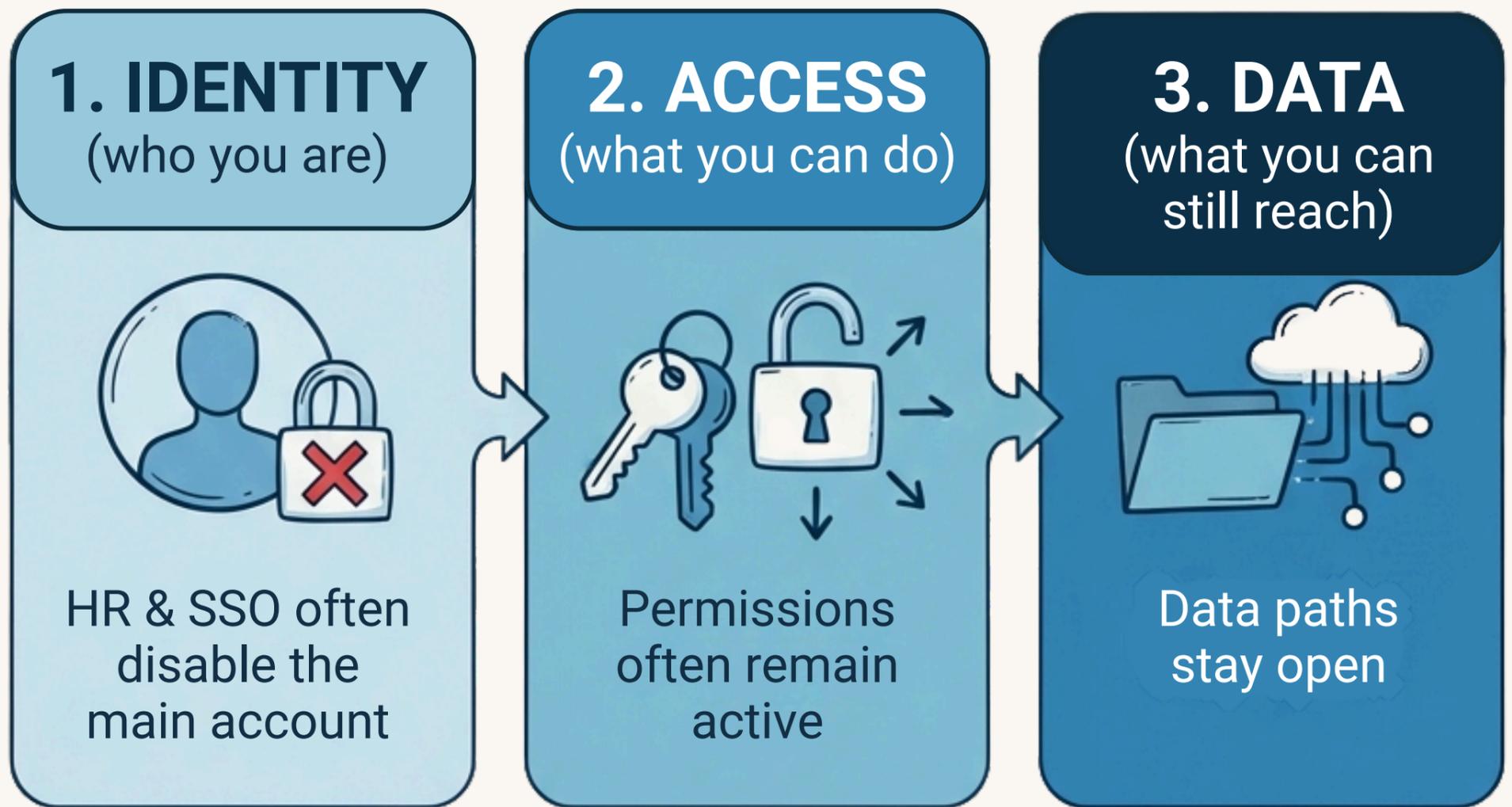
In healthcare, education, nonprofits

Identity gets shut off

Shared
Finance
App

Permissions and data paths don't

Wylie Blanchard

The predictable misses Anything outside SSO

Shared drives (patient/student records)

Finance approval system

Vendor portals tied to old inboxes

Cloud apps authenticated outside SSO

Collaboration history & sensitive chats

Local accounts bypassing HR

Wylie Blanchard
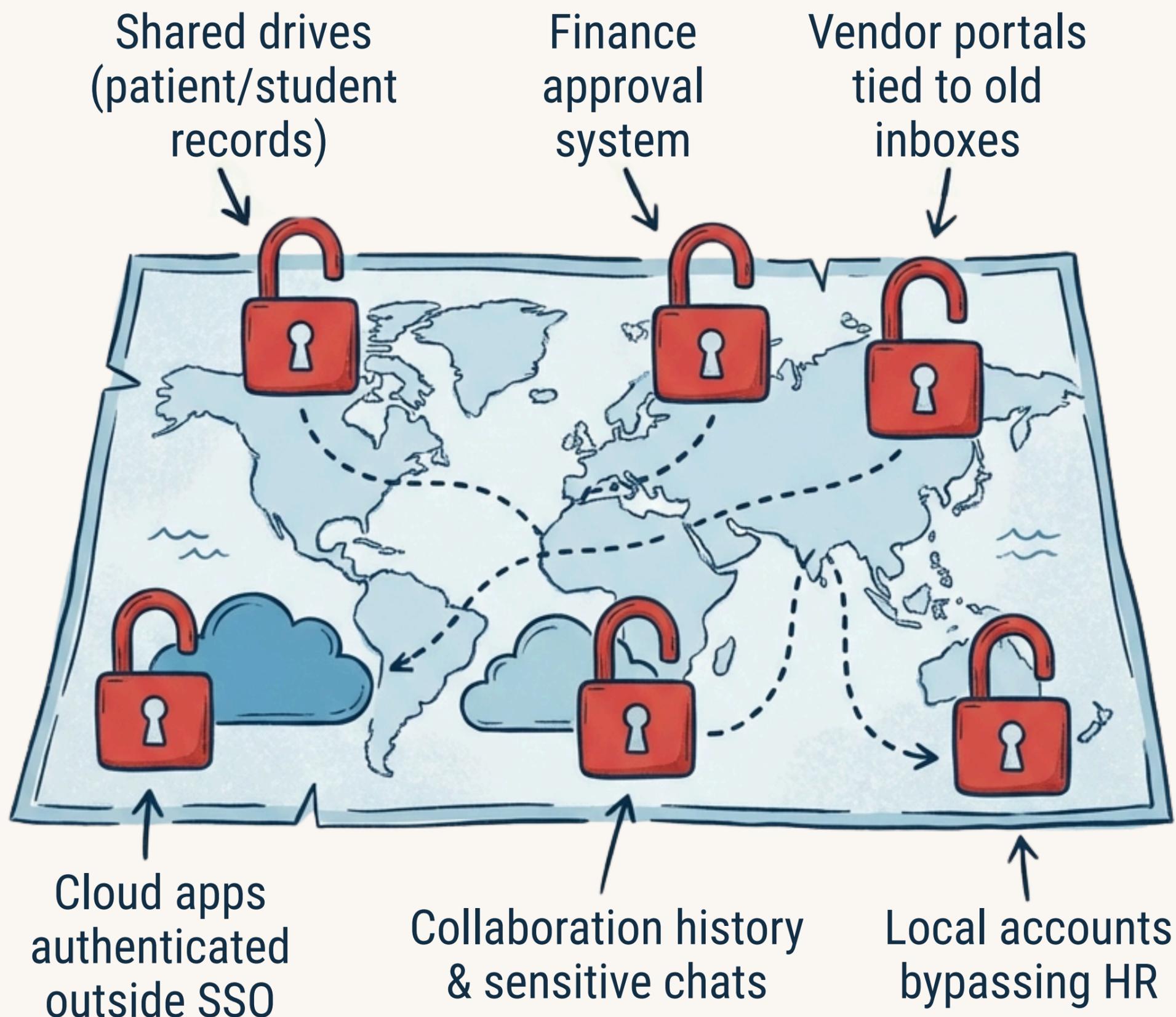
The 90-Day Audit (The Reality Check)

1. Pull your last 90 days of terminations

2. Pick your top 10 critical systems
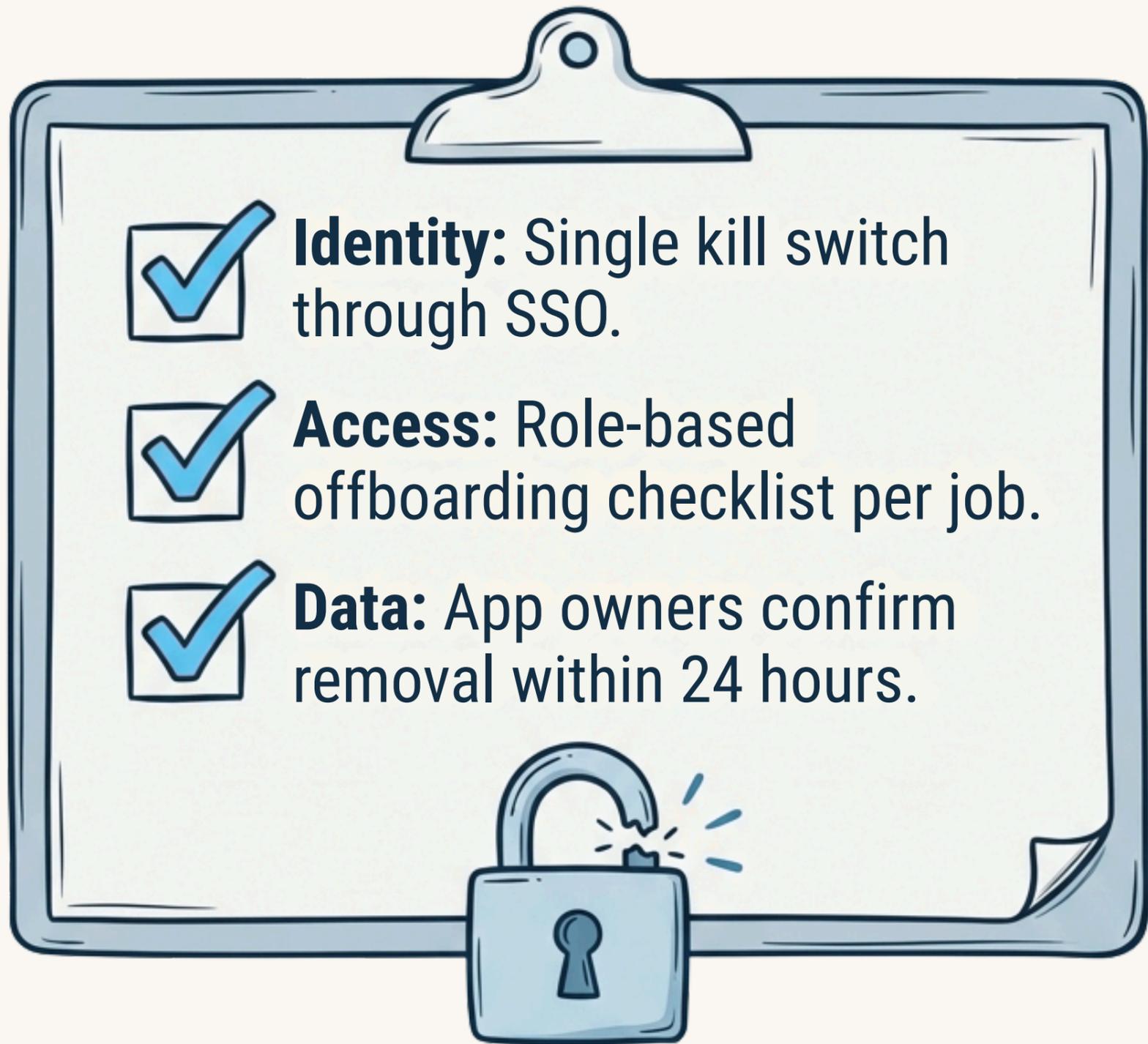
3. Pull last-login reports for those terminated users
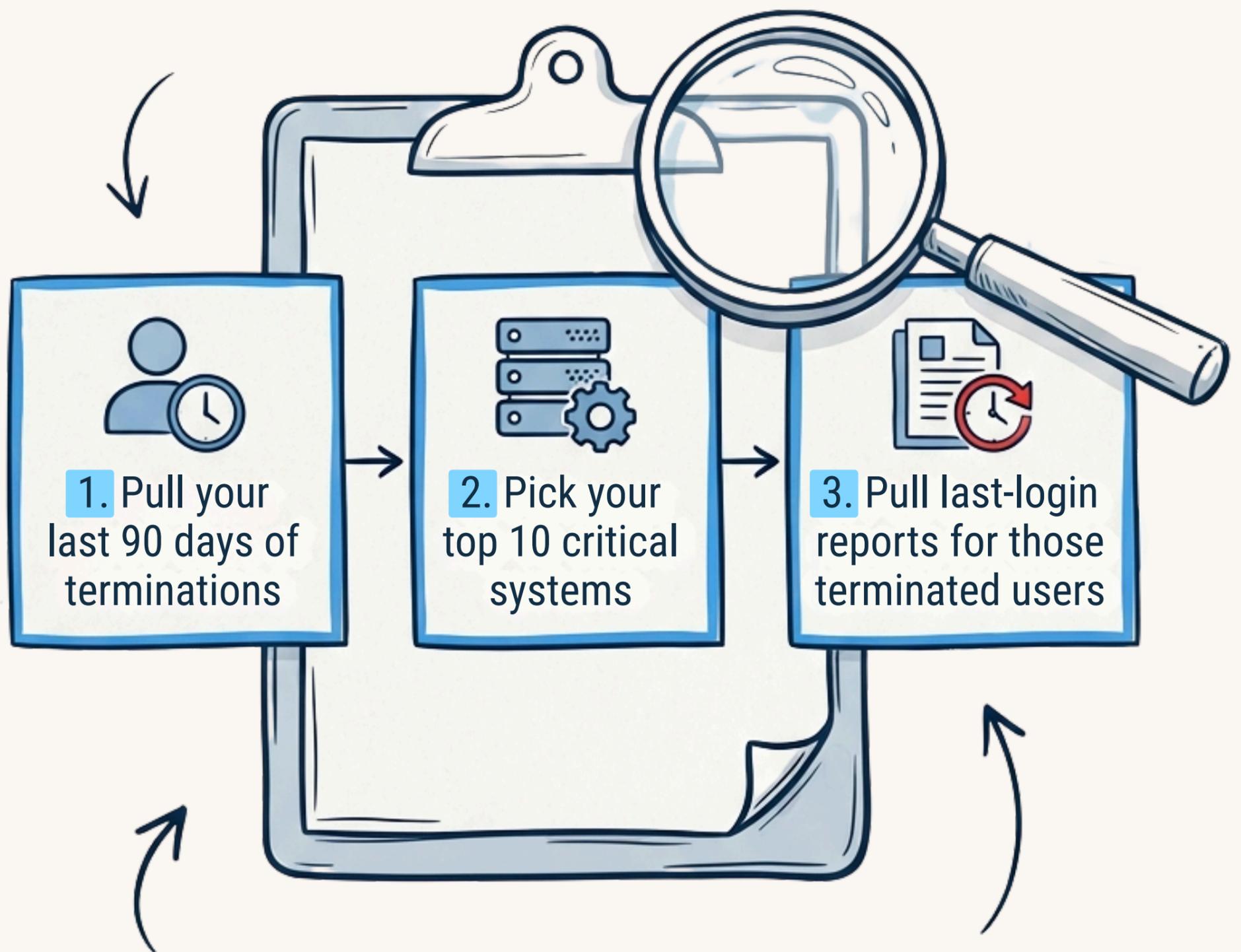
If anyone logged in after their exit date, you have a control gap

(If you can't pull a last-login report, that's a finding too.)

Wylie Blanchard

Close the gap with a simple mechanism

Identity: Single kill switch through SSO.

Access: Role-based offboarding checklist per job.

Data: App owners confirm removal within 24 hours.

Comment OFFBOARD below and I'll DM you the audit steps + the role-based checklist template