1. Problem Statement: Solving "Permission Bloat" and Production Anxiety

In modern cloud environments, identities (users and services) are often granted **"Admin" or excessive permissions** to ensure developers aren't blocked while building. Over time, this creates **"Permission Bloat"**, where 90% of granted access is never actually used.

The core challenge is **The Production Paradox**: Security teams want to remove unused permissions to stay safe (Least Privilege), but they are paralyzed by the **fear of breaking a live application**. Currently, engineers lack a "Confidence Score" or a way to test the impact of removing a permission before actually deleting it. This leads to a massive, unmanaged security risk that is too scary to fix manually.

---

2. User Persona: Kunal, the Cloud Security Engineer

Profile: Kunal is responsible for securing hundreds of microservices. He is technically elite but overwhelmed by the scale of cloud permissions.

His Goals:

- **Implement Least Privilege:** Ensure no user has more "keys" than they need for their daily job.
- **Zero Downtime:** Harder the system without ever causing a "403 Forbidden" error for a legitimate service.

His Pain Points:

- **Information Overload:** He sees thousands of "Unused Permission" alerts but doesn't know which ones are safe to delete and which are "rare but critical" (e.g., for monthly backups).
- **Manual Effort:** He spends hours chasing developers on Slack to ask, *"Do you still need this?"* only to get "I'm not sure" as an answer.
- **High Stakes:** If he deletes the wrong permission, he is the one responsible for the system outage.