IAM Permissions Explorer

Problem Statement

Cloud IAM environments accumulate permissions over time through roles, groups, inherited policies, and service-wide access.This results in excessive permissions. Security and platform teams lack clear visibility into who has access and why it exists on their usage and risks involved. This creates security risk and audit friction. The IAM Permission Explorer solves this by providing a clear and navigable view of effective permissions across - services, users, groups, and roles.

User Persona

As a Cloud Security or Platform Engineer I want to access and modify the the IAM Policies and follow the compliance standards and file auditory reports. They need a fast and reliable way to understand access identify unused or risky permissions and take corrective action without breaking production systems.

Figma Files

https://www.figma.com/design/2flzfP2u8AoSX8Qe9jfEyJ/Untitled?node-id=0-1&t=5XD2Horq3PgfBD9i-1

Features - Prioritized

P0 – Core Visibility & Control (Must Have / MVP)

- A unified IAM dashboard organized into **Services, Roles, Groups, and Users**, allowing admins to switch views without losing context.
- The **Services view** acts as the primary control plane where admins can view each service individually, see what access exists, and understand **who has access and why**.

- Each service panel clearly shows **groups, roles, and users** with access, while explaining whether access is **direct or inherited**.
- Users who have **direct access not coming from a group or role** are shown separately to highlight potential risk.
- Admins can edit service-level settings such as **default expiry rules and access behavior** directly from the service dashboard.

P1 – Access Remediation & Risk Reduction

- Admins can manually **revoke all unused access** for a service by defining or overriding inactivity thresholds, especially useful during incidents or emergency lockdowns.
- Each service can trigger **MFA re-verification** for all users associated with sensitive or risky permissions.
- The **Users view** provides a full picture of a user's effective access, including their groups, roles, and attached policies or services.
- For every user permission, the system shows the **last used date**, helping admins decide what can be safely revoked.
- Permissions can be **manually edited or revoked** at the user, group, or role level with clear visibility into impact.

P2 – Automation & Governance

- A scheduled **cron job continuously evaluates service usage**, identifying unused permissions based on each service's defined rules.
- Unused access is automatically revoked or flagged according to service-specific thresholds, reducing long-term permission sprawl.
- All access changes and usage checks are logged to maintain traceability and audit readiness.

P3 – Audit & Compliance Enablement

- A dedicated **Audit Reports** section generates compliance-ready reports using access logs and modification history.

- Reports focus on **least-privilege enforcement**, unused access removal, and access change accountability.
- Enables faster internal and external audits with minimal manual intervention.

Success Metric

1. Reduction In Excessive/ Unused Permissions

- % decrease in unused permissions over time (e.g. unused for 30/60/90 days)
- Number of permissions revoked or expired via the tool
- Reduction in direct (non-inherited) user permissions

2. Time to Identify and Fix Risky Access

- Average time from identifying a risky permission to revoking or expiring it
- Time taken to answer “Who has access to X and why?”

3. Reduced Audit Effort

- Time spent preparing IAM audit reports
- Number of manual IAM data pulls during audits
- Audit findings related to excessive access (before vs after)

4. Confidence in Access Changes

- Ratio of permissions reviewed vs ignored
- Frequency of bulk actions (revoke unused access, MFA re-verification)
- Low rollback rate after revocations