**1. Conditional Access Based on User Attributes (ABAC)**

**Scenario:**

User **John (Global Entitlement)** from the **UK** tries to access **India Data**.

**User Attributes (from AD or IDM):**

* Role: Global Analyst
* Country: UK
* Data Access Flags: malaysia\_access = false, india\_access = false

**Logic Applied at Middleware/API Layer:**

typescript

CopyEdit

if (user.role === 'Global Analyst' && data.country === 'India') {

if (user.india\_access) {

allowAccess();

} else {

denyAccess('Approval needed for India data access');

}

}

**Result:**

* John is denied unless india\_access = true is set by a local data owner.

**2. Dynamic Approval at Data Access Level**

**Scenario:**

User **Jane** needs to access **Malaysia payroll reports** through the dashboard.

**Implementation:**

* When Jane clicks the report:
  + A popup says: *"Access to Malaysia data requires approval. Request now?"*
* Upon confirmation:
  + A request is sent to **Malaysia Data Owner** for approval.
  + Upon approval, Jane gets access for **7 days**.

**Outcome:**

* Access to data is not automatic despite entitlement.
* Approvals are tracked outside RSAM.

**3. Country-Specific Access Logs & Review Mechanism**

**Scenario:**

User **Ali** (with global entitlement) accessed India’s vendor data 3 times last week.

**Setup:**

* Logging system captures:
  + Username
  + Timestamp
  + Dataset accessed
  + Country of data

**Dashboard (for India DPO):**

| **Username** | **Accessed Country** | **Date** | **Dataset** |
| --- | --- | --- | --- |
| Ali | India | 2025-04-01 | Vendor Payments |
| Ali | India | 2025-04-03 | Vendor Master |
| Ali | India | 2025-04-04 | Vendor Master |

**Outcome:**

* India has complete visibility.
* Can raise a flag if something looks suspicious.

**4. Hybrid RBAC with Global Entitlement Override**

**Scenario:**

User **Rachel** has a global entitlement. However, access to **Malaysia** data requires an additional role.

**Roles:**

* Global\_Entitlement
* Malaysia\_Approved\_Access (assigned only after request)

**Access Check:**

typescript

CopyEdit

if (user.hasRole('Global\_Entitlement') && dataset.country === 'Malaysia') {

if (user.hasRole('Malaysia\_Approved\_Access')) {

allowAccess();

} else {

denyAccess('Missing Malaysia approval role');

}

}

**Outcome:**

* Rachel submits a one-time request.
* Once the Malaysia team approves, she’s granted the override role.

**5. Just-in-Time (JIT) Access for Country Data**

**Scenario:**

User **Mike** wants access to India sales data for a project.

**Flow:**

* Mike clicks: *"Request JIT Access to India Data"*
* A form opens:
  + Purpose: *"Sales Forecasting"*
  + Duration: *"48 hours"*
* India team receives notification and grants access via internal portal.
* Access token expires after 48 hours.

**Backend Access Logic:**

typescript

CopyEdit

if (user.hasActiveJITAccess('India')) {

allowAccess();

} else {

denyAccess('Request JIT access first');

}

**Outcome:**

* No permanent access.
* Temporary access only when justified and approved.

**6. API Gateway Rule Enforcement**

**Scenario:**

APIs are used to fetch India/Malaysia records.

**Gateway Policy (JSON example):**

json

CopyEdit

{

"rule": "country-data-restriction",

"conditions": [

{

"if": "user.global\_entitlement == true && data.country == 'India'",

"then": "requireHeader('X-India-Access-Approved')"

}

],

"errorMessage": "Access to India data requires specific header approval."

}

**What Happens:**

* If the required header is missing or incorrect:
  + The API gateway **blocks the request**.
* This header can only be added by backend services after verifying approval.

**Outcome:**

* No changes to RSAM or frontend.
* Access is centrally controlled and logged.

**Summary Table**

| **Option** | **Method** | **Access Control Mechanism** | **Example Outcome** |
| --- | --- | --- | --- |
| 1. ABAC | Attributes check | User's flags must allow country | Denied access unless flag true |
| 2. Dynamic Approval | Just-in-time request | Popup approval before access | Temporary access after approval |
| 3. Logging | Access review | Transparent logging of access | Countries audit and monitor |
| 4. Hybrid RBAC | Role override | Requires extra role for each country | Access only if override exists |
| 5. JIT Access | Temporary grant | Request & auto-revocation | 24-48 hr access only |
| 6. API Gateway | Policy enforcement | Conditional headers or IPs | API blocks unauthorized requests |