Understanding Access Control Models in Cybersecurity

Who gets access to what – and why it matters

Understanding Access Control Models: The Foundation of Cybersecurity

In cybersecurity, **access control** is like the bouncer at a club. It determines who gets in, where they can go, and what they can do. It's the critical first line of defense for protecting sensitive data.

Access Control: More Than Just a Password

It's the process of restricting access to network resources, applications, and data.

It involves three key steps:

- **Identification**: Who are you?
- **Authentication**: Prove it! (e.g., password, biometrics)
- **Authorization**: What are you allowed to do?

Key Access Control Models

Four widely used models in cybersecurity:

- Discretionary (DAC)
- Mandatory (MAC)
- Role-Based (RBAC)
- Attribute-Based (ABAC)

DAC: Discretionary Access Control

Owner decides who gets access

Pros: Highly flexible

Cons: Prone to human error (e.g., over-sharing)

Example: File sharing permissions

Best for: Small teams, low-risk data

MAC: Mandatory Access Control

System enforces strict rules

Pros: Very high security

Cons: Rigid, complex to manage

Example: Government/military systems

Best for: Highly classified environments

RBAC: Role-Based Access Control

Access based on **job roles**

Pros: Simplifies management

Cons: Role creep if not audited

Example: HR sees payroll, IT sees servers

Best for: Large organizations

ABAC: Attribute-Based Access Control

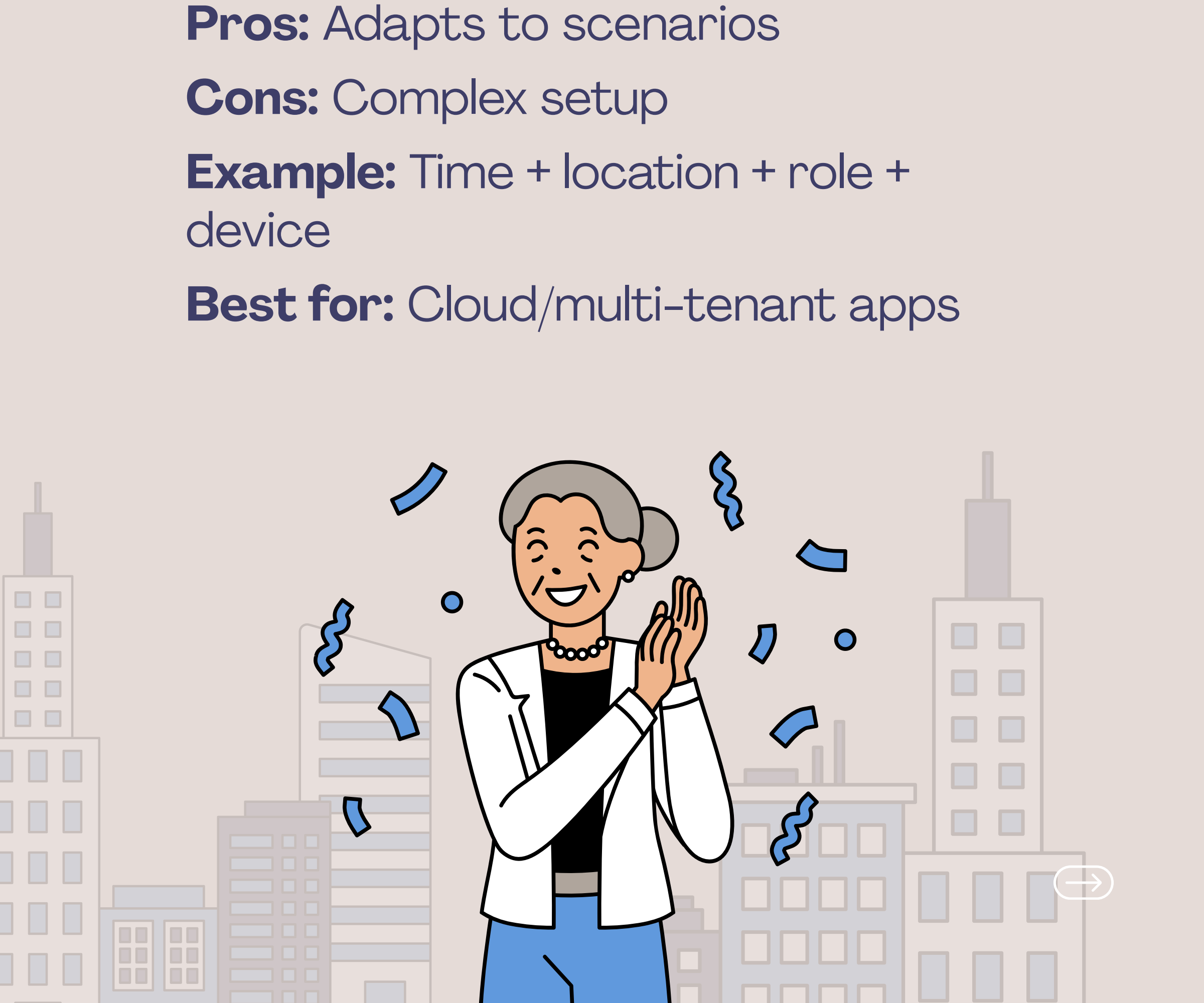
Multiple factors determine access

Pros: Adapts to scenarios

Cons: Complex setup

Example: Time + location + role + device

Best for: Cloud/multi-tenant apps



Which Model is Right for You?

The best model depends on your organization's needs.

Model	Flexibility	Security	Complexity	Best For
DAC	★★★★★	★★	Low	Teams
MAC	★	★★★★★	High	Classified
RBAC	★★★	★★★★	Medium	Corps
ABAC	★★★★	★★★★★	High	Dynamic

5 Steps to Better Access Control

Audit current permissions

Map user roles clearly

Implement least privilege principle

Monitor access patterns

Review permissions regularly

Summary

- 🚀 Access control is the backbone of security
- ✅ Right model = balance between security & usability
- 🔒 Build a layered defense strategy

If you found this carousel helpful, don't forget to like, comment, and share so others can also **let's build a stronger, security-aware community.**

Saikat Rakshit