Policy-Based Access Control

Securely connecting identities to digital assets, powered by Policy Based Access Control (PBAC)

PBAC: Going Beyond RBAC and ABAC

RBAC, while historically useful, has proven limitations with scalability and flexibility. ABAC attempted to solve this, but brought additional administrative overhead which most organizations cannot effectively manage, especially across an ever-expanding and diversifying technology stack. Additionally, both methods lack the identity context needed to continuously establish trust at every stage of a digital interaction.

Policy-Based Access Control (PBAC) fills this gap with its advanced, agile, policy-driven approach, dynamically responding to changes, and efficiently catering to the nuanced demands of modern access control scenarios.

What is Policy-Based Access Control (PBAC)?

Simply, PBAC is a strategy for controlling user access to systems. Permissions are determined by combining natural language and business logic with attributes, roles, conditions, and contextual signals (e.g. risk score, threat intelligence). It enables organizations to rapidly adapt access to changes in business and security requirements. This can include changes in user demand, productivity, privacy, and regulatory compliance.

PBAC tackles challenges that conventional access control models struggle with. It has the ability to respond to changes occurring along digital interactions by factoring in elements such as identity-context, location, time, type of resource, and more. PBAC's flexibility enables enterprises to continuously evolve with security standards, provide efficient data access control, strengthen data security, and ultimately reduce risk.

Business Impact

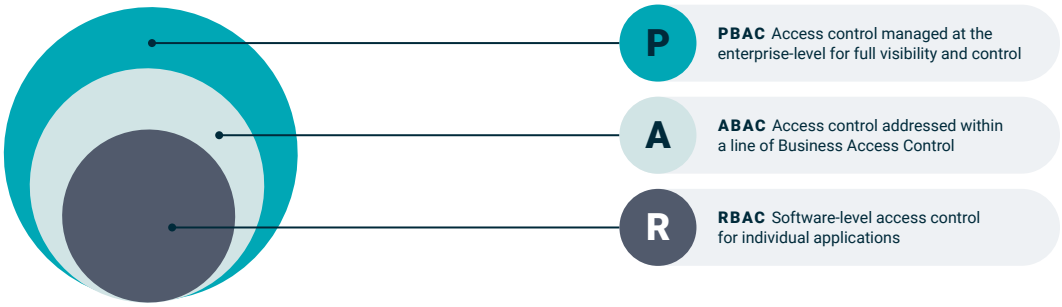
ENHANCED BUSINESS AGILITY
Provide an efficient authorization management approach, simplifying the development lifecycle and accelerating time to market.

ROBUST SECURITY
Bolster a Zero Trust model through dynamic, fine-grained, and real-time authorization decisions. Apply identity-aware context through architecture layers.

FULL VISIBILITY AND CONTROL
Gain granular control of access to sensitive data, allowing for better regulation people and systems interactions with resources.

ENTERPRISE SCALABILITY
Apply a more comprehensive and unified approach, addressing the needs of the entire enterprise technology stack, from apps to APIs, microservices, and data.

The Evolution of Enterprise-level Access Control



The Differences between PBAC, RBAC, and ABAC

Unlike traditional access control methods, PBAC offers an advanced, adaptable, and context-aware authorization mechanism, making it an excellent choice for businesses with intricate and evolving access needs. The selection among PBAC, RBAC, and ABAC should be based on the specific requirements and context of an organization.

	PBAC	RBAC	ABAC
MAIN CONCEPT	Decides access based on policies incorporating roles, and attributes, and real-time context when necessary.	Decides access based on roles assigned to users.	Decides access based on attributes associated with users, resources, and the environment.
FLEXIBILITY	HIGH Can handle complex scenarios with dynamic and context-aware decisions.	MODERATE Can handle different job functions but lacks adaptability for complex scenarios.	HIGH Can handle complex scenarios with granular control through attributes.
EASE OF MANAGEMENT	Depends on complexity of policies. Can be complex for very dynamic scenarios.	Simple due to role-based assignment of permission, but suffers from siloed approaches.	Depends on the number and complexity of attributes, as well as how policies are authored.
SCALABILITY	HIGH Can scale with business and security requirements.	MODERATE Scalability can be challenging with numerous roles and permissions.	MODERATE TO HIGH Scalability depends on the complexity and quantity of attributes.

ABOUT PLAINID

PlainID, the Authorization Company, simplifies the complexity businesses face when securely connecting identities to digital assets. Powered by PBAC, PlainID provides a SaaS-based, centralized policy management platform with decentralized enforcement to manage who can access what across the enterprise technology stack; including applications, data, API, microservices and more. Visit PlainID.com for more information.

plainID