PlainID Role & Entitlement Manager

Improve your IAM posture, take control over all entitlements, and support Zero Trust Architecture withan advanced authorization solution

PlainID's Role & Entitlement Manager bridges the historically strict and inflexible world of Entitlements with Policy Based Access Control, putting context and giving visibility into access decisions so that IT Professionals and Application Owners can get a clear view of who is authorized to do what across all organizational assets in today's complex business environment. Add it to your current IAM implementation, or use as a standalone for your coarse grain entitlement requirements, and leverage a PBAC model for the ultimate in efficiency, security and ROI. You still build traditional roles, but with Role & Entitlement Manager they are built upon Policies. It focuses on "The Decision," giving companies the ability to manage the most complex or the largest access requirements. This 'Single Source of Truth' contains, along with access entitlements, the business context that is essential to build a dynamic access authorization model.

"It has become our "golden record" for all access decisions.We no longer have to look into each application to understand who has access to what"

-IAM Professional at large European Bank

Why Entitlement & Role Manager?

Comprehensive life cycle management for all access entitlements, including roles, security groups, and applications

Shared responsibility and accountability over access between the line of business and IT through automated processes

Governance by policies goes beyond Identities, keeps the focus on assets, functionality &usability

Zero Trust Architecture enforced, using contextual data to make access decisions on a need-to-know basis

Proactive approach to compliance needs even for newly added applications, identities and assets

Data and privacy concerns are met, providing full visibility as to who has access to what and why
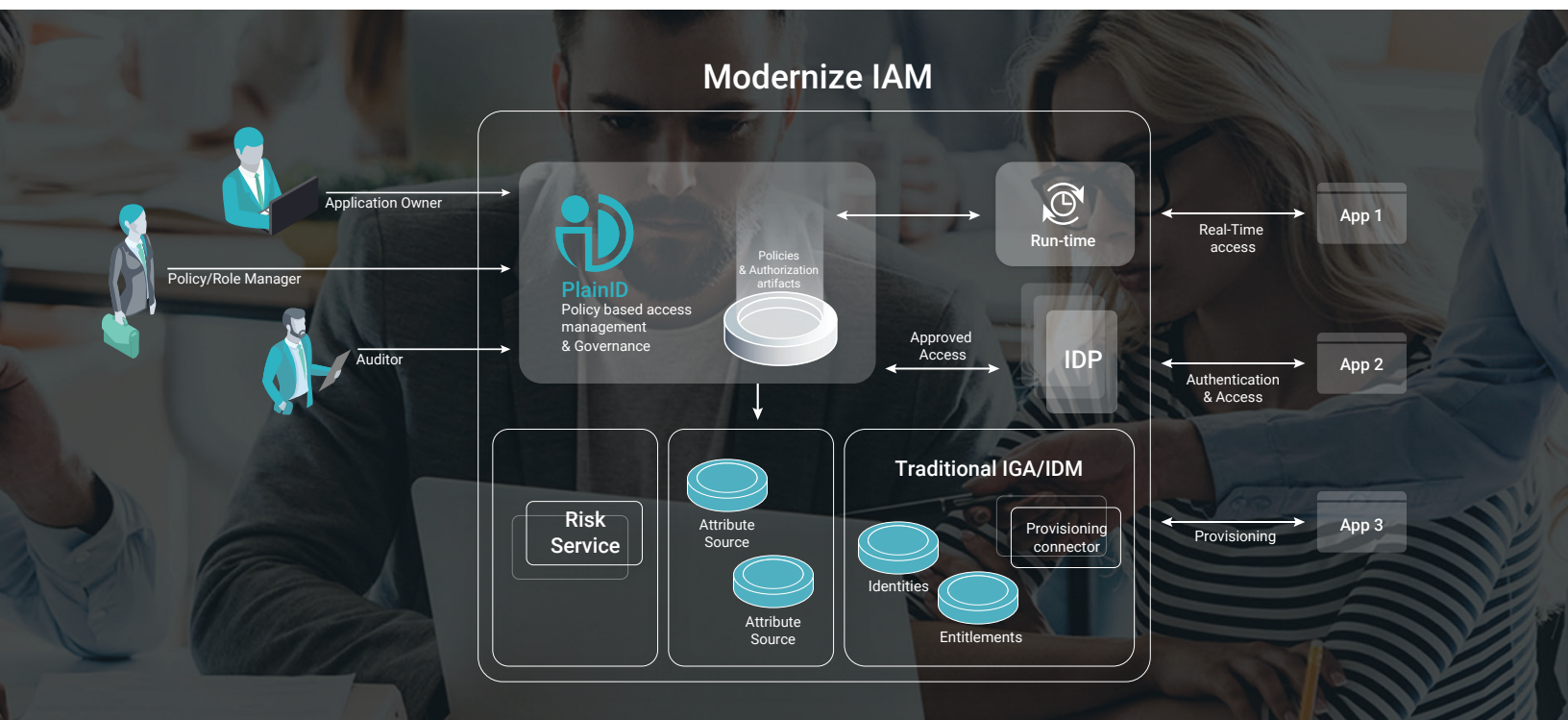
Fast path to IAM through self-services for application owners

Connects with existing IGA tools and Applications

Features & Benefits

- Entitlement Catalog
- Entitlement Lifecycle Management
- Role Management
- Entitlement Enrichment
- Approval Workflows

- Flexible Schema
- Delegation of Administrative Rights
- Version Control
- Application On-boarding
- App Self Registration

- Advanced Analytics
- Compliance & SOD control
- Visibility and Investigation
- Policy & Role mining
- Graphical UI & REST API

Modernize IAM

Application Owner

Policy/Role Manager

Auditor

PlainID
Policy based access management & Governance

Policies & Authorization artifacts

Run-time

IDP

Approved Access

Real-Time access → App 1

Authentication & Access → App 2

Provisioning → App 3

Risk Service

Attribute Source

Attribute Source

Traditional IGA/IDM

Identities

Entitlements

Provisioning connector

PBAC Platform

The PBAC Platform provides a focused approach to Authorization Management and control. Among the platform benefits are:

Enterprise grade solution: Our platform provides the set of capabilities required to efficiently manage your access decisions including a full life-cycle management of application entitlements (fine and coarse grained), delegated admin rights to improve collaboration, audit logs and versions control, business workflows and more

Built for the business and IT: Our platform connects the technical world of entitlements to the business world of access policies by visualizing all entitlements (fine and coarse-grained) with their business meaning, therefore bringing awareness into both worlds

Unified experience: Browsing through entitlements from any business application, or mining for access policies, is done under a unified web interface with different access levels based on the person's role in the organization

Modularity of deployment: Offers flexibility; start your project by mining for access policies, or begin by bring context and visibility into access entitlement at any level from any business application

Integration with external tools such as IGA/IDM systems and access enforcement tools is done through industry-standard APIs to further connect between disparate IAM systems, thus modernize your overall IAM program today