Modern Access Control for APIs

Identity-aware security, powered by Policy-Based Access Control (PBAC)

Challenges in API Access Control

According to OWASP API Security Top 10, eight of the top ten gaps in API security are related to insufficient access controls. The explosion of external services supporting everything from B2B, B2C, B2B2C, and remote workforce has created a new landscape for bad actors to exploit.

API access control faces significant challenges, particularly when it comes to Broken Object Level Authorization (BOLA) and Broken Object Property Level Authorization (BOPLA) — a common vulnerability that leads to unauthorized data access or manipulation. BOLA and BOPLA arises when APIs fail to adequately verify whether a user or service is authorized to access a specific object, such as a database entry, or resource and its elements.This oversight allows attackers to exploit object IDs or access paths to sensitive data – exposing organizations to compliance risks.

Unlike traditional API access control, which may broadly grant access to an API endpoint, object-level authorization requires fine-grained, context-aware policies to ensure that every request is appropriately validated against the user's permissions. It's no longer sufficient to use coarse grain claims to trigger an API. We must base authorization on the user or service being allowed to take action against the specific digital asset and its properties that are serviced through that API.

Modernize & Improve API Security To Move at the Speed of Business

Today's fast-paced digital economy demands API security solutions that can adapt quickly to evolving business needs while safeguarding sensitive data. The **PlainID Platform™**, provides fine-grained and dynamic access policies for API gateways and microservices. PlainID Authorizers™ provide out-of-the-box integration that simplifies authorization across the enterprise.

Make the Complex Simple: The complexity of the API gateway and microservice layer requires the use of Policy Based Access Control allowing you to decouple the simplicity of business policies from the complexity of the technical implementation. This means that you can simplify the centralized management of Business logic and policies that map back to the API and microservices.

Accelerate Time to Market: PlainID enables you to onboard new APIs with their business controls faster, and adapt to changing business requirements without requiring any engineering efforts. Organizations can gain the agility they need to meet modern business demands. Allowing Security to be an enabler not a blocker.

Business Impact

Support Modern Architecture
Meet your organization's API-first business strategy and user experience.

Minimize Risk With Identity-First Security
Address Zero Trust and continuous authorization in real-time.

Better Manage API Access To Policies
Secure APIs through a single pane of glass with a central management platform

Accelerate Time To Market
A user-friendly GUI saves your developers' time and resources.

Technical Insight

Pairing PlainID Authorizers at the API gateway and microservices layers creates a multi-layered security approach:

- **API Gateway Layer:** Enforces fine-grained API access control, blocking unauthorized API requests.
- **Microservices Layer:** Applies fine-grained policies, securing individual data objects and operations.

This dual-layer approach prevents unauthorized access, mitigates BOLA & BOPLA risks, and enhances overall API security.

Key Components of PlainID's Modern Access Control for APIs

Identity-aware Controls: Extend the identity information beyond what's in the API transaction to support context based authorization decisions.

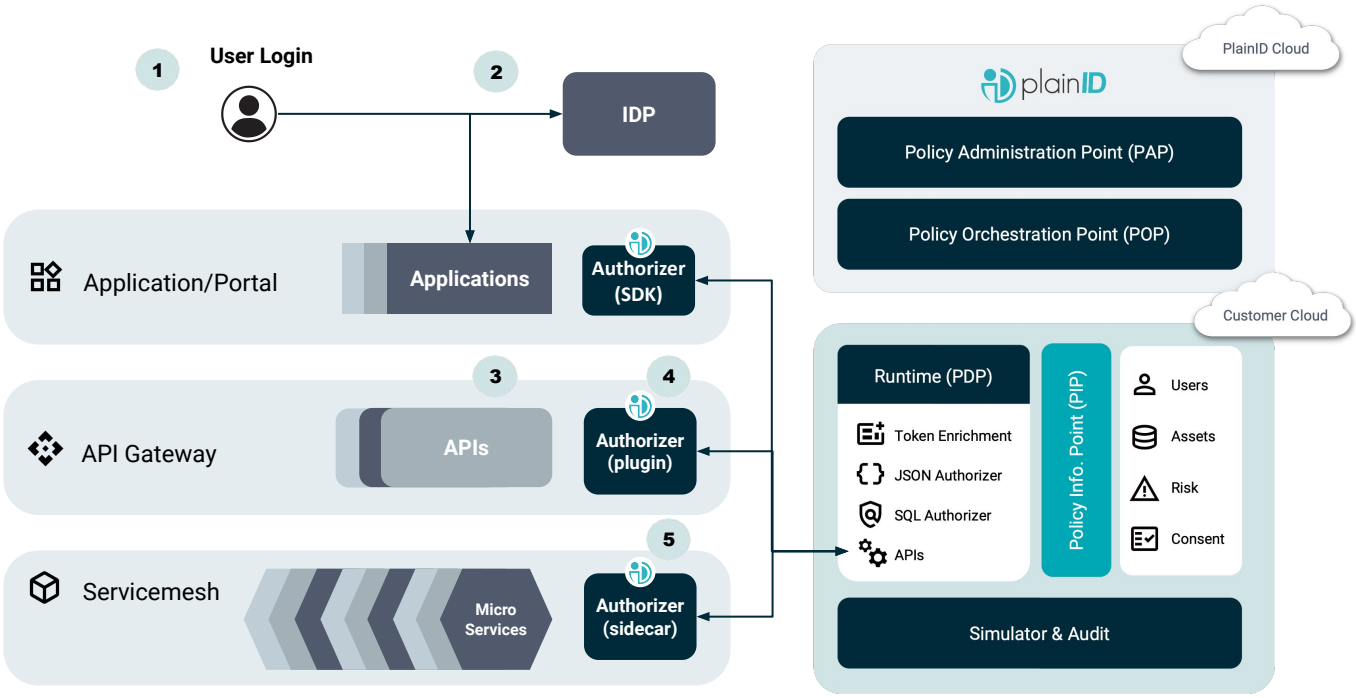
Business-driven API Policies: Consolidate large number of APIs to fewer business driven policy definitions, allowing simpler onboarding of new services.

API Mappers: Map API endpoints to their digital assets by linking JSON objects, JWT attributes, and full URIs to policy building blocks, unifying multiple endpoints into a single logical structure.

Out-of-the box PlainID Authorizers™: Integrate all leading API gateways and services mesh, allowing faster time to value in implementing identity-first security following least privilege principles.

Solution Architecture

1. User logs into the application
2. Application sends authentication request to the Identity Provider (IdP)
3. The application sends API calls directed through the API Gateway to access different services
4. PlainID's Authorizer (implemented as a plugin in the API Gateway) receives the request and makes a dynamic access decision in real-time, based on the policies. The decision can permit/deny the transaction OR equip the transaction with token exchange/ enrichment for additional identity-aware permissions.
5. The API call is passed on to the service layer



Azure API Management · envoy · Kong · apigee · Amazon API Gateway · MuleSoft · Istio · WSO2

ABOUT PLAINID

PlainID is the world's leading provider of enterprise Authorization, helping enterprises address the complex challenges of Identity Security. The PlainID Platform allows you to discover, manage, and authorize access control policies for enterprise applications and data. Our solution is architected to protect against identity-centric security threats powered by Policy-Based Access Control (PBAC). Visit PlainID.com for more information.

plainID