

Dynamic Data Masking for JSON

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

Identity-Aware Security for JSON Objects

JSON is widely used for data transmission across enterprise ecosystems, but enterprises often lack the robust data security controls applied to traditional databases.

Traditionally, authorization has been handled within individual, homegrown applications, an approach that lacks scalability and security. Siloed controls and disparate rules create challenges in enforcing consistent authorization, complicating data security and compliance as data usage expands.

PlainID solves these issues by centralizing authorization through the **PlainID Authorization Platform** and **PlainID Authorizer™ for JSON**. This approach enforces tailored controls on JSON objects moving across microservices, APIs, and end applications securing your digital assets. The Authorizer addresses Broken Object Level Authorization (ensuring users can view, edit, create, or delete only permitted digital assets) and Broken Object Property Authorization (restricting access to specific attributes within those assets).

Improve Security & Reduce Developer Overhead

The **PlainID Authorizer™ for JSON** enforces runtime data masking and data redaction, delivering only data permitted by granular, identity-aware policies. It extends database security paradigms to JSON, APIs, and microservices, allowing both object- and attribute-level access control with dynamic masking.

Applications often fetch data using service accounts with broad permissions, leaving developers responsible for masking sensitive data at the API or middleware level—a practice that can create inconsistencies and vulnerabilities. PlainID addresses this by integrating its Authorizer™ for JSON with Envoy filters, Apigee flows, Azure API policies, and similar technologies in API gateways, to automatically intercept and filter data in JSON form which reduces developer responsibility and minimizes security gaps. PlainID enforces policies that consider identity-aware context (e.g. risk, location, role) – ensuring only necessary and authorized data is accessible to each user.

Business Impact



Central Policy Management

Manage access to data, delivered via JSON objects with a business-driven UI to provide consistent access decisions across enterprise apps.



Coarse and Fine-Grained Authorization

Enforce fine-grained controls at a granular level by determining what objects/object properties and data are exposed to the authorized user.



Low/No-Code Integration

Easy to call Microservice that returns fully authorized JSON object or pair with API gateways and service meshes for code-free interception and enforcement.



Consistent Data Control

Employs REST APIs to extend robust access control consistently across data, applications, and microservices.

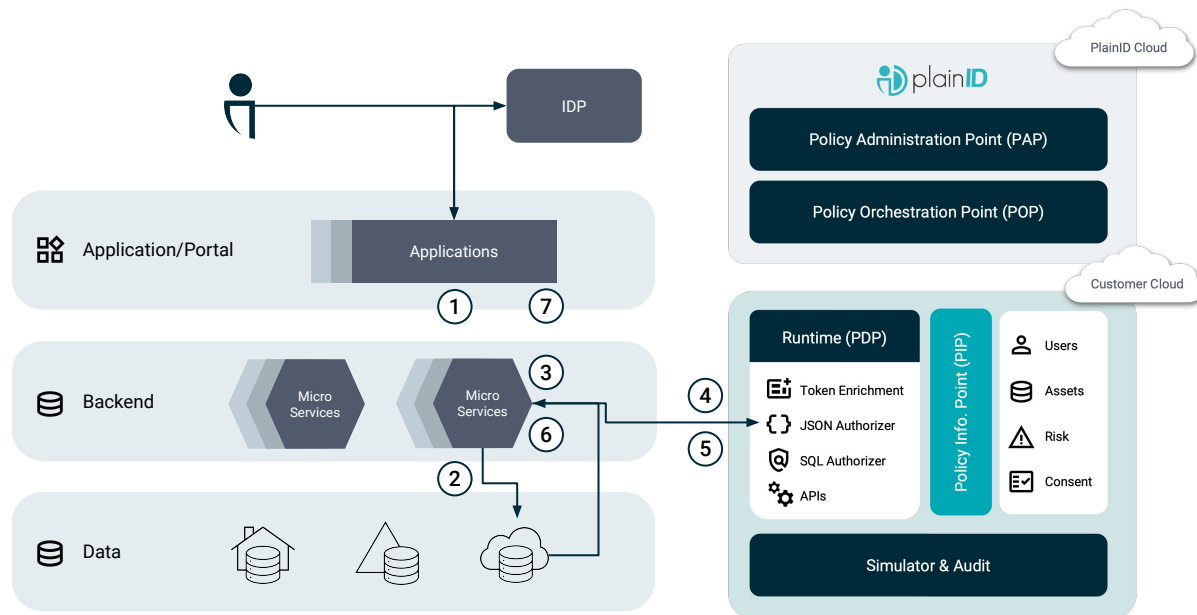


Technical Insight

PlainID Authorizers™ for JSON and SQL Databases enable layered data security by filtering at different stages:

- The Authorizer for SQL adjusts the query to pre-filter data rows, while JSON applies post-filtering to limit specific object properties.
- Together, they ensure that only authorized data is accessed, adding depth to data protection.

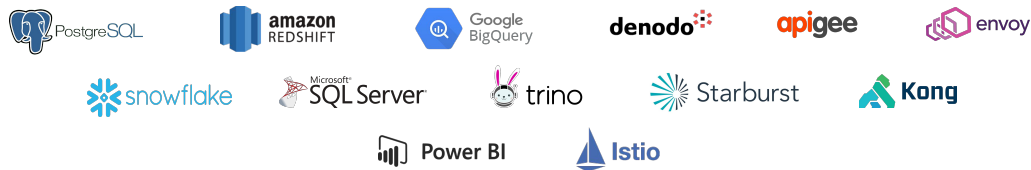
How the PlainID Authorizer™ for JSON Data Works



1. A user goes to application and login via the IDP to request data.
2. The microservice fetches the data from the data repository.
3. The microservice gets the data back and forms the JSON object(s) to be return to the application.
4. The microservice send the JSON objects to the PlainID JSON Authorizer.
5. The PlainID JSON Authorizer redacts/masks Objects and Object properties dynamically based on PlainID's policy evaluation.
6. The PlainID JSON Authorizer returns authorized Objects to the microservice.
7. The microservice returns the Object to the Application and user.

Future-proof Your Enterprise

The **PlainID Integration Hub** is designed to address the complex challenges of enterprise access control. By offering out-of-the-box Authorizers™ and Integrations, it allows for a standardized approach across varied and distributed infrastructures – unifying disparate access controls under one platform.



Visit PlainID.com/integration-hub for more information

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.