WHITEPAPER

Securing Complex Enterprise Ecosystems at Scale with Dynamic Authorization

plainID

Table of Contents

Introduction

The digital age has spurred unprecedented growth and innovation across various sectors, but it has also significantly expanded the attack surface for cyber threats. As enterprises continue to digitize their operations, the complexity and sophistication of cyberattacks have evolved – making cybersecurity a top priority.

One of the most alarming trends in this landscape is the prominence of unauthorized access, which accounted for approximately 70% of all data breaches in 2022. This statistic underscores the critical vulnerabilities enterprises face in securing their digital assets and the importance of robust authorization capabilities.

The Growing Importance of Authorization in Cybersecurity

Authorization is crucial in the cybersecurity ecosystem, acting as the gatekeeper for accessing sensitive information and critical systems. Authorization determines who is allowed to access what information, under what circumstances, and with what limitations. As cyber threats have become more sophisticated, dynamic and context-aware authorization mechanisms are essential to ensuring secure access. Traditional models of authorization, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), are pushed to their limits by the demands of modern IT environments such as cloud infrastructure, microservices, and APIs.

Authorization determines who is allowed to access what information, under what circumstances, and with what limitations.

Evolving Threat Vectors and Their Impact on Authorization

Bad actors continuously develop new strategies and techniques to exploit vulnerabilities in IT systems, and these exploits and techniques have shifted to identity-based attacks. Some of the evolving threat vectors that have a direct impact on authorization include:

- **Insider Threats:** Malicious insiders or compromised user accounts with excessive permissions can abuse authorized access to leak, modify, or destroy sensitive data.
- **API Vulnerabilities:** APIs have become the backbone of software development but can also introduce significant security risks if not properly authorized
  and secured, leading to data breaches.
- **Microservice Architectures:** While offering scalability and flexibility, microservices increase the complexity of authorization as each service may require its own set of access controls.
- **Cloud Application Misconfigurations:** The shift to using more SaaS applications has expanded the attack surface, where misconfigurations across controls native to the SaaS applications can lead to unauthorized access to cloud-stored data and resources.

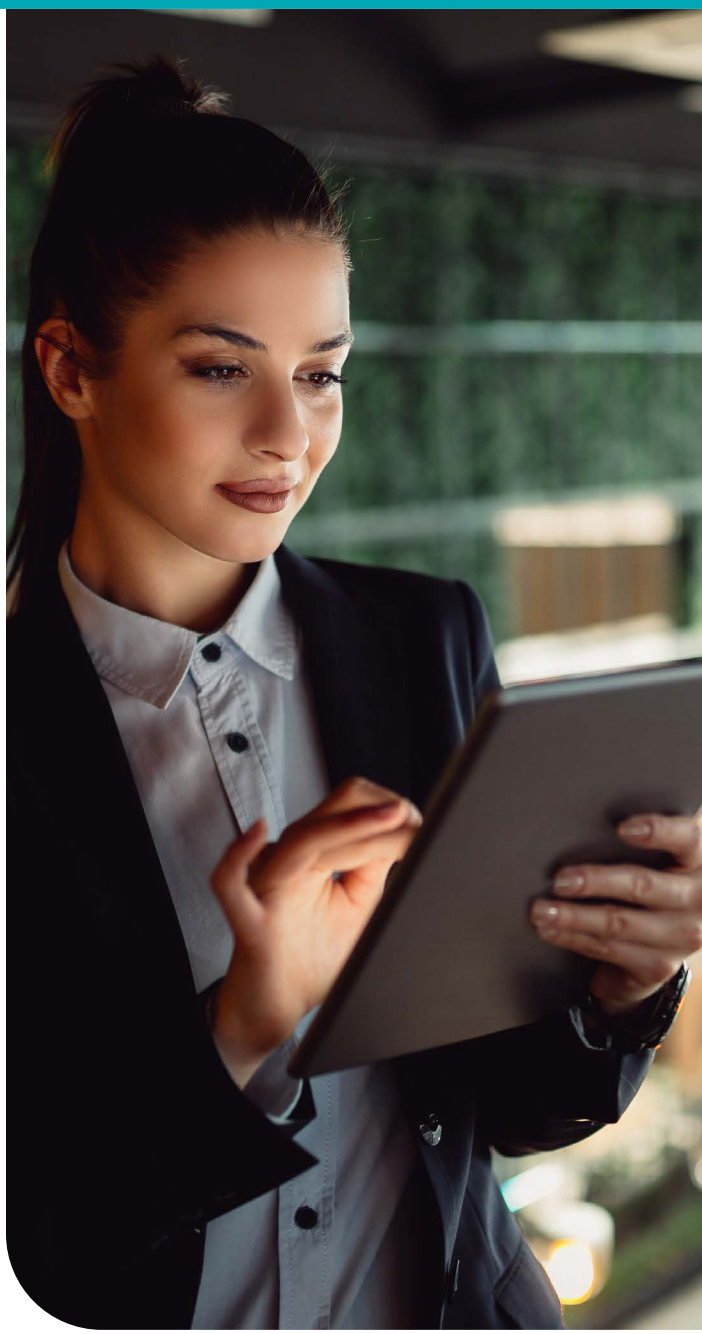
The critical nature of these threats highlights the necessity for enterprises to adopt more advanced and flexible authorization strategies that can adapt to the changing cybersecurity landscape and protect against unauthorized access.

The Urgency for Advanced Authorization

The statistic that unauthorized access was responsible for 70% of all data breaches in 2022 is a stark reminder of the importance of securing access to digital assets. This necessitates a shift towards more dynamic and context-aware authorization mechanisms that evaluate access requests in real-time, taking into account various attributes and risk signals. Policy-based Access Control (PBAC), sometimes referred to as Policy-based Access Management, approaches and solutions, such as Dynamic Authorization, offer the flexibility, scalability, and granularity needed to address these evolving threats effectively.

As cyber threats continue to evolve, so must the strategies and technologies we employ to defend against them. The high incidence of data breaches due to unauthorized access underscores the need for a paradigm shift in how enterprises approach authorization within their cybersecurity frameworks.

Why Dynamic Authorization and PBAC Matter to Enterprises



The Significance of Dynamic Authorization

Dynamic Authorization represents a paradigm shift in access control. Unlike static methods that evaluate permissions based solely on predefined roles or attributes, Dynamic Authorization assesses each access request in real-time. It takes into account various contextual factors—such as the user's location, device, time of day, and the sensitivity of the requested data—to make informed decisions about granting or denying access. This real-time evaluation enables enterprises to respond swiftly to emerging threats and changing conditions and thereby enhances security and operational flexibility.

PlainID's Dynamic Authorization Service uses a Policy-Based Access Control framework to exemplify this approach. This framework enables enterprises to define and manage access policies centrally, using natural language and graphical interfaces that non-technical stakeholders can easily understand and interact with. PBAC simplifies policy management and ensures that access decisions are consistently applied across the entire digital landscape, from applications and APIs to microservices and the data layer.

Going Beyond RBAC and ABAC Limitations with PBAC

RBAC and ABAC, while foundational, have limitations in a rapidly evolving digital environment. RBAC's role-based permissions can become cumbersome to manage as enterprises scale and roles diversify. ABAC offers granularity but at the cost of increased complexity and difficulty in policy management. PBAC addresses these challenges by integrating the strengths of RBAC and ABAC within a unified, policy-driven framework. It offers the granularity of ABAC with the manageability of RBAC, plus the added flexibility of dynamic, real-time decision-making based on contextual information.

By adopting PBAC, enterprises can achieve a balance between security, usability, and compliance. Policies can be easily updated to reflect new business requirements or regulatory changes without the need for extensive coding or system reconfiguration, facilitating business agility and resilience.

Enabling a Zero Trust Security Model

The principle of "never trust, always verify" lies at the heart of the Zero Trust security model. Dynamic Authorization and PBAC are instrumental in implementing this model, as they allow for continuous verification of access requests, regardless of where they originate or what resources they target. PlainID's approach ensures that authorization decisions are made based on up-to-date policies and real-time assessments of risk, thereby minimizing the attack surface and reducing the potential for unauthorized access.

In essence, Dynamic Authorization and PBAC provide the foundation for a more secure and adaptable authorization strategy, crucial for enterprises seeking to protect their digital assets in a perimeterless world. By leveraging PlainID's Dynamic Authorization Service, enterprises can enhance their security posture, ensure compliance, and facilitate the seamless operation of their digital ecosystems, all while adhering to the principles of Zero Trust.

PlainID's Solution: Centralized Policy Management with Dynamic Authorization

PlainID's approach to access control addresses the multifaceted challenges of modern IT environments. By integrating Dynamic Authorization capabilities with a centralized policy management framework, PlainID provides a robust and flexible solution that caters to the evolving needs of digital enterprises.

Overview of PlainID's Approach to Solving Modern Access Control Challenges

PlainID recognizes the complexity and dynamic nature of access within modern IT ecosystems, which are characterized by cloud services, microservices architectures, APIs, and a diverse array of user devices and roles. In response, PlainID moves beyond the limitations of traditional access control models like RBAC and ABAC, by introducing a more agile and intelligent way to manage access rights across an organization's entire digital landscape.

The core of PlainID's solution is its ability to dynamically authorize access requests in real-time, using a comprehensive set of policies that consider various contextual factors. This approach ensures that access rights are granted based on the most current conditions and user attributes, thereby enhancing security and operational efficiency.

Features of PlainID's Dynamic Authorization Service and PBAC Framework

- **Centralized Policy Management:** PlainID's PBAC framework allows for centralizing policy management, enabling administrators to define and update access policies from a single location. This centralized approach simplifies the governance of access rights and ensures consistency across all digital assets.

- **Dynamic Authorization:** Leveraging real-time decision-making capabilities, PlainID's service dynamically evaluates access requests against the set policies, considering the context of each request. This ensures access rights are appropriately granted or denied based on current conditions and risk levels.
- **Graphical Policy Editor:** PlainID provides a user-friendly policy editor to facilitate easy policy creation and management. This tool allows business and non-technical stakeholders to contribute to policy definition using natural language and graphical interfaces, democratizing access control management.
- **Seamless Integration:** PlainID Authorizers™ seamlessly integrate with an organization's existing IT infrastructure, including gateways, services, directories, databases, applications (custom and SaaS CoTS), and cloud services. This interoperability ensures that PlainID's dynamic authorization capabilities can be extended enterprise-wide without disrupting existing workflows.

Benefits of Centralized Policy Management and Dynamic, Real-Time Authorization Decisions

- **Enhanced Security:** PlainID's solution significantly reduces the risk of unauthorized access and data breaches by making access decisions based on real-time data and contextual information. The dynamic nature of authorization ensures that access rights are always aligned with the latest security policies and threat intelligence.
- **Operational Efficiency:** Centralized policy management eliminates redundancies and inconsistencies in access control mechanisms, streamlining administrative processes. This efficiency reduces the workload on IT teams and speeds up the deployment of new applications and services.
- **Regulatory Compliance:** PlainID's solution facilitates the granularity and auditability of access controls, helping enterprises meet compliance requirements with global, local, and industry-specific regulations. The ability to quickly adapt policies in response to changing legal landscapes further strengthens compliance postures.
- **Improved User Experience:** Dynamic authorization ensures that users have access to the resources they need when they need them, without unnecessary friction. This balance between security and convenience improves overall user satisfaction and productivity.

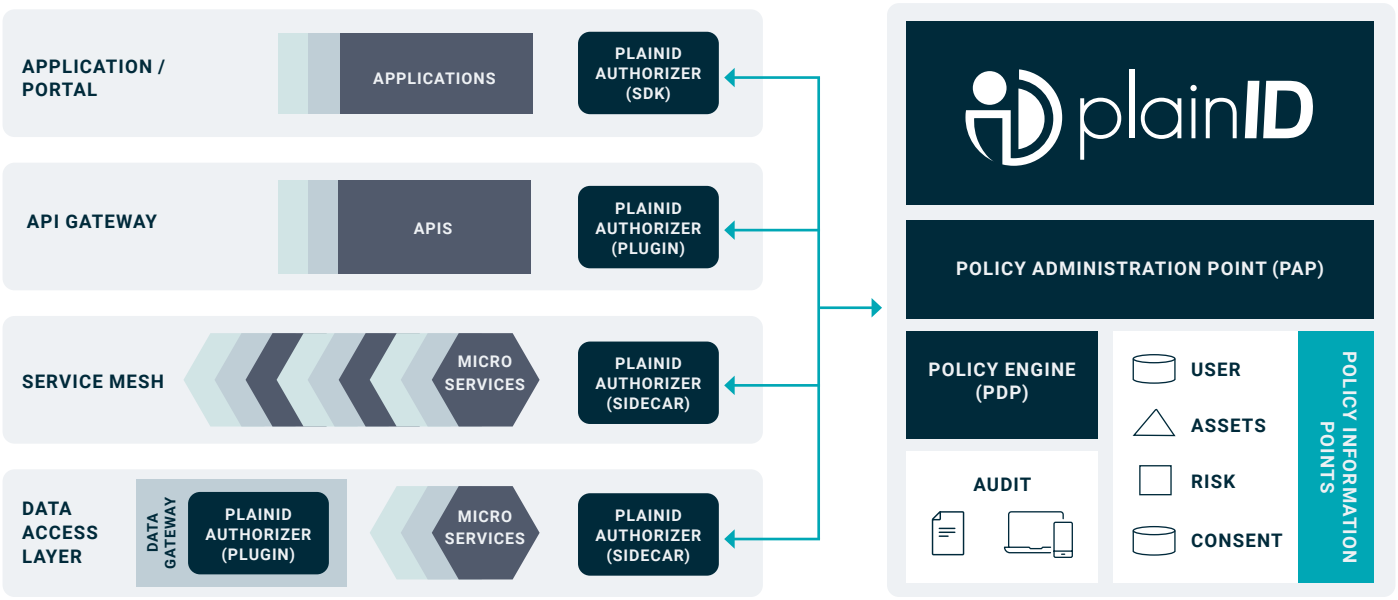
PlainID's solution to access control challenges presents a comprehensive, intelligent, and flexible approach to managing authorization in modern IT environments. By centralizing policy management and employing dynamic, real-time authorization decisions, enterprises can enhance their security posture, operational efficiency, and compliance efforts, all while providing a seamless user experience.

PlainID's Dynamic Authorization Service Architecture and Authorizers

PlainID's Dynamic Authorization Service is engineered with a robust and scalable architecture that underpins its sophisticated policy-based access control (PBAC) framework. Central to this architecture are the PlainID Authorizers, which play a pivotal role in implementing dynamic and context-aware authorization across an organization's digital assets. This section delves into the architectural components and the functionality of Authorizers within the PlainID ecosystem.

Key Components of PlainID's Dynamic Authorization Service Architecture

The architecture of PlainID's Dynamic Authorization Service is designed to be highly adaptable, ensuring seamless integration with existing IT infrastructures while providing comprehensive access control capabilities.



The architecture is composed of several key components:

Policy Decision Point (PDP): The Policy Decision Point is at the heart of the architecture, which is responsible for making real-time authorization decisions. The PDP evaluates access requests against the defined policies, considering the current context and attributes associated with each request.

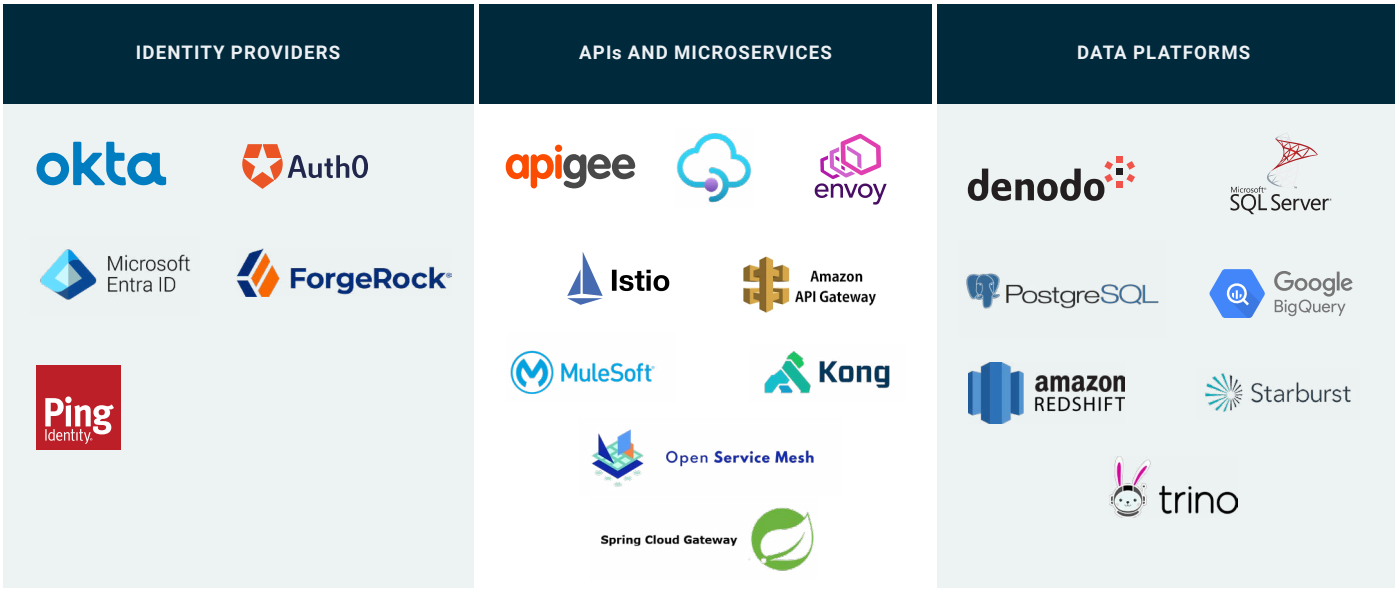
Policy Administration Point (PAP): The Policy Administration Point provides a centralized interface for creating, managing, and updating access policies. Utilizing a user-friendly graphical interface, the PAP enables technical and non-technical stakeholders to define access rules and policies.

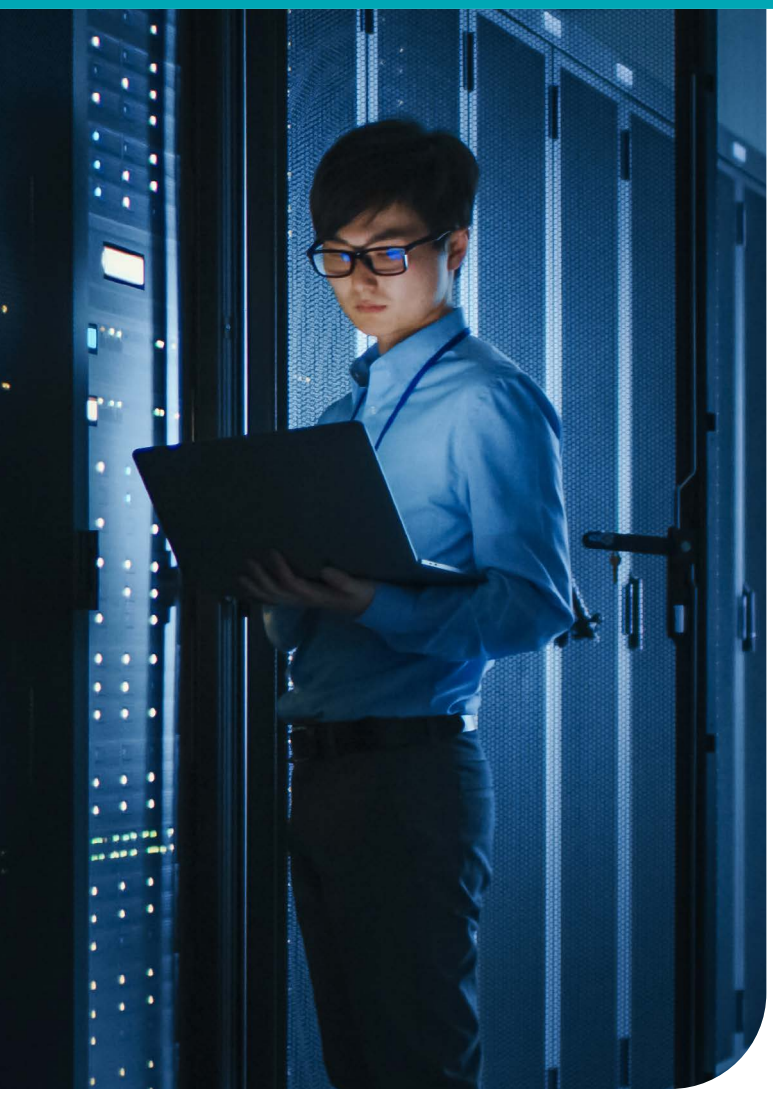
Policy Information Point (PIP): This component retrieves relevant attribute data from various sources within the organization's IT environment. The PIP supplies the PDP with the necessary contextual information and attributes required to make informed authorization decisions.

PlainID Authorizers (PEP): Located at the access request points within the system, the Policy Enforcement Point intercepts access requests and forwards them to the PDP for evaluation. Once a decision is made, the PEP enforces it by granting or denying access based on the PDP's decision.

The Role of PlainID Authorizers in the Dynamic Authorization Service

PlainID Authorizers are specialized modules within the service architecture that facilitate the integration of dynamic authorization capabilities with various types of digital assets, including applications, APIs, microservices, and data stores. Authorizers act as the glue or bridge between the PEP and the specific resources (and technology) requiring access control, ensuring access policies are enforced consistently and effectively across the entire digital ecosystem.





Application and API Authorizers: These Authorizers are designed to secure applications and APIs by managing access permissions in line with the policies defined within the PAP. They ensure that only authorized requests can interact with protected endpoints, thereby safeguarding sensitive operations and data.

Microservice Authorizers: Given the distributed nature of microservices architectures, these Authorizers provide fine-grained access control, ensuring that services can only be accessed by authenticated and authorized entities. This is crucial for maintaining the integrity and security of microservices-based applications.

Data Layer Authorizers: To protect the data layer, these Authorizers control access to databases, data warehouses, and other data storage solutions. They enforce policies that dictate who can read, write, or modify data, aligning access rights with compliance requirements and business needs.

Each type of Authorizer is tailored to integrate seamlessly with its target environment, leveraging standard protocols and APIs to intercept access requests and apply the appropriate policies. This design allows PlainID's Dynamic Authorization Service to extend its policy-driven access control capabilities across the diverse components of an organization's IT landscape, providing a unified and consistent approach to authorization.

In summary, the architecture of PlainID's Dynamic Authorization Service, complemented by its versatile Authorizers, offers a comprehensive solution for managing access control in a dynamic and complex digital environment. This architecture not only enhances security and compliance but also facilitates operational efficiency by centralizing policy management and automating the enforcement of access decisions across various platforms and technologies

Each type of Authorizer is tailored to integrate seamlessly with its target environment, leveraging standard protocols and APIs to intercept access requests and apply the appropriate policies.

PlainIDs Dynamic Authorization Service Through the Technology Stack

For a more technical deep dive into the examples provided for PlainID's Dynamic Authorization Service, let's explore how each solution can be enhanced by integrating specific aspects of PlainID's capabilities. This will illustrate how enterprises can apply these solutions more effectively.

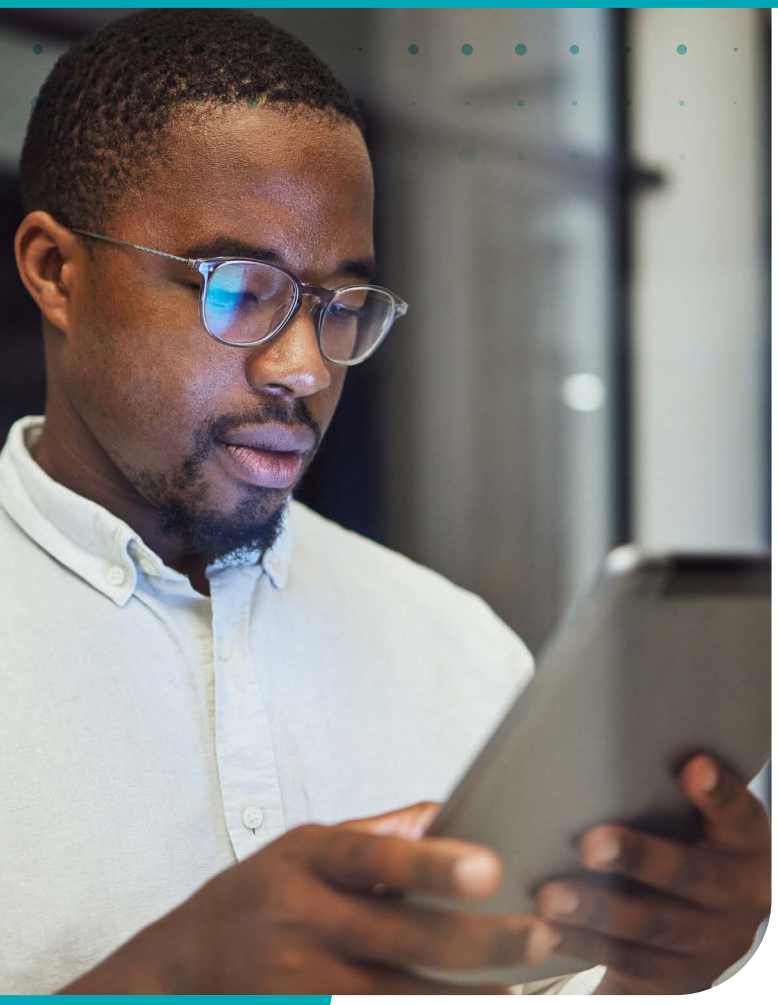
Application Access Control with PlainID SDK

Integrating PlainID's SDK into application development enables nuanced and tighter access control by leveraging PlainID's dynamic authorization capabilities directly within the application logic. PlainID can also be integrated with the Identity Provider (IDP), allowing dynamic control over the OAUTH claims provided to the application and allowing control over authorization.

Here are ways access control for applications can be applied:

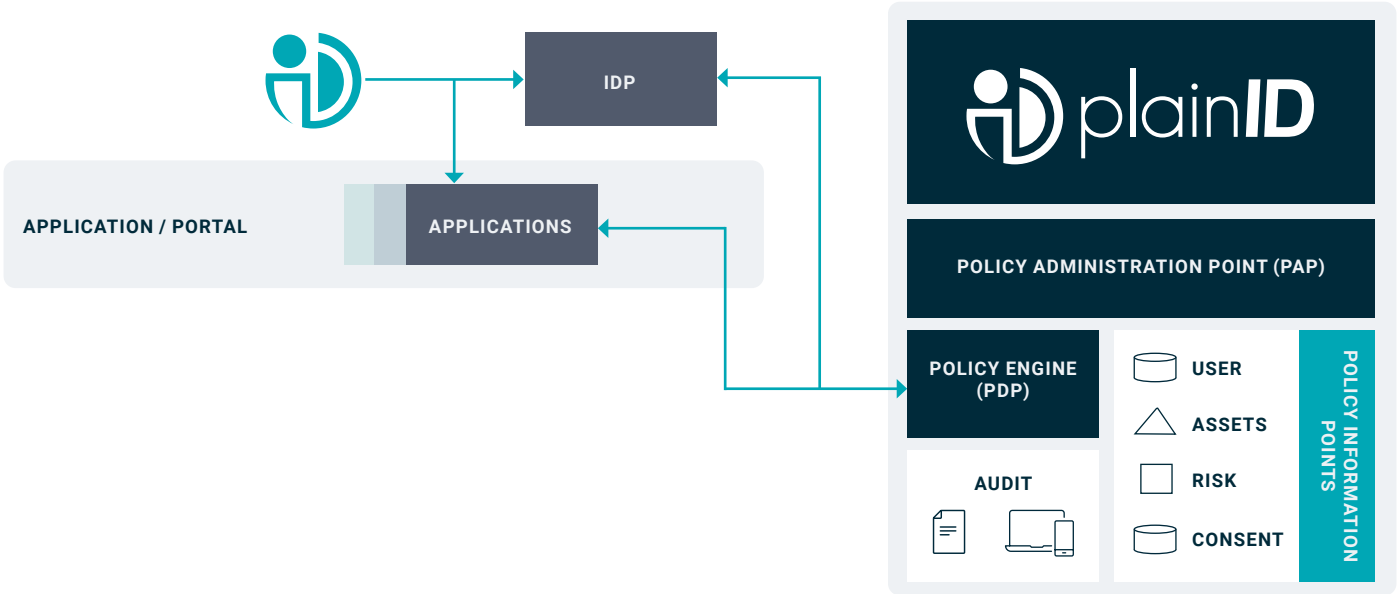
SDK Integration: Developers can embed PlainID's SDK into the application's backend, ensuring all access requests are intercepted and evaluated against the central policy hub. This allows for real-time, context-aware access decisions without significant overhead.

IDP Integration: If an application is currently using claims-based Authorization and is integrated with a company's IDP, PlainID can be used to dynamically control the enrichment of OAUTH tokens, deciding in real time which claims should or should not be included in the Access or Identity token. In essence, this also controls the application's dynamic authorization.



Dynamic Policy Evaluation: Access decisions are made dynamically, considering the context of the request, including user attributes, roles, location, and time of day. For instance, access to a financial record within an application could be restricted based on the user's role and the data's sensitivity, with policies dynamically updated in PlainID's Policy Administration Point (PAP) reflecting immediately in application behavior.

Real-time Updates and Scalability: As business requirements evolve, policies can be updated in real-time through PlainID's management console, ensuring the application adapts to new access control needs without deployment downtime.

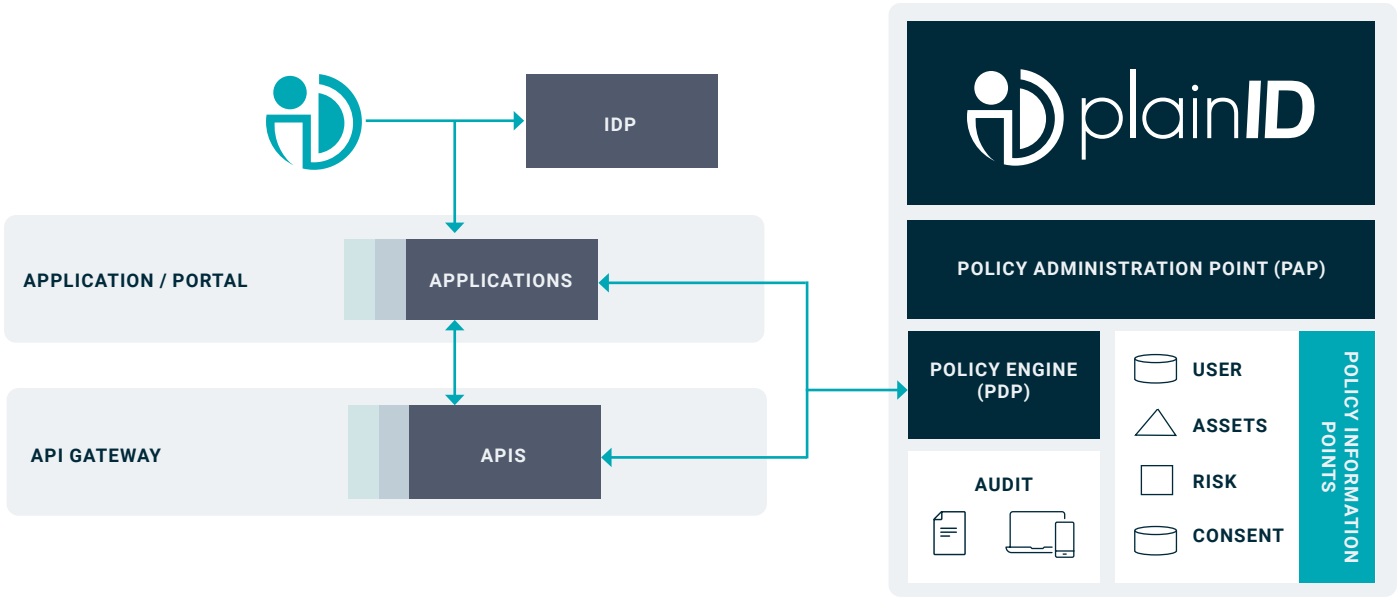


API Gateway Authorization with PlainID

For securing API gateways, PlainID's solution can be strategically positioned to augment existing API management platforms such as Apigee and AWS API Gateway.

Here are ways access control for API gateways can be applied:

- **Policy Enforcement:** By integrating with PlainID, API gateways can enforce granular access control policies that are centrally managed. This setup ensures that API requests are consistently authorized across all services, leveraging PlainID's dynamic authorization to evaluate access based on comprehensive policy rules.
- **Mitigating OWASP API Security Risks:** To address issues such as broken object level authorization, PlainID can assess the context of each API call, including the calling user's permissions and the specific data or object being accessed, ensuring that users can only access objects they are explicitly authorized to. PlainID enhances security by implementing context-aware authorization checks that take into account the specific object a user is attempting to access through an API call. By integrating with the application's backend and API gateway, PlainID can intercept API requests and apply dynamic authorization logic that evaluates not just who is making the request but also enforces protection on the digital asset they are trying to retrieve or modify through the API.
- **Scalable and Secure API Exposure:** With PlainID, policies governing API access are centrally managed and dynamically enforced, allowing enterprises to securely expose new services at scale without compromising security.

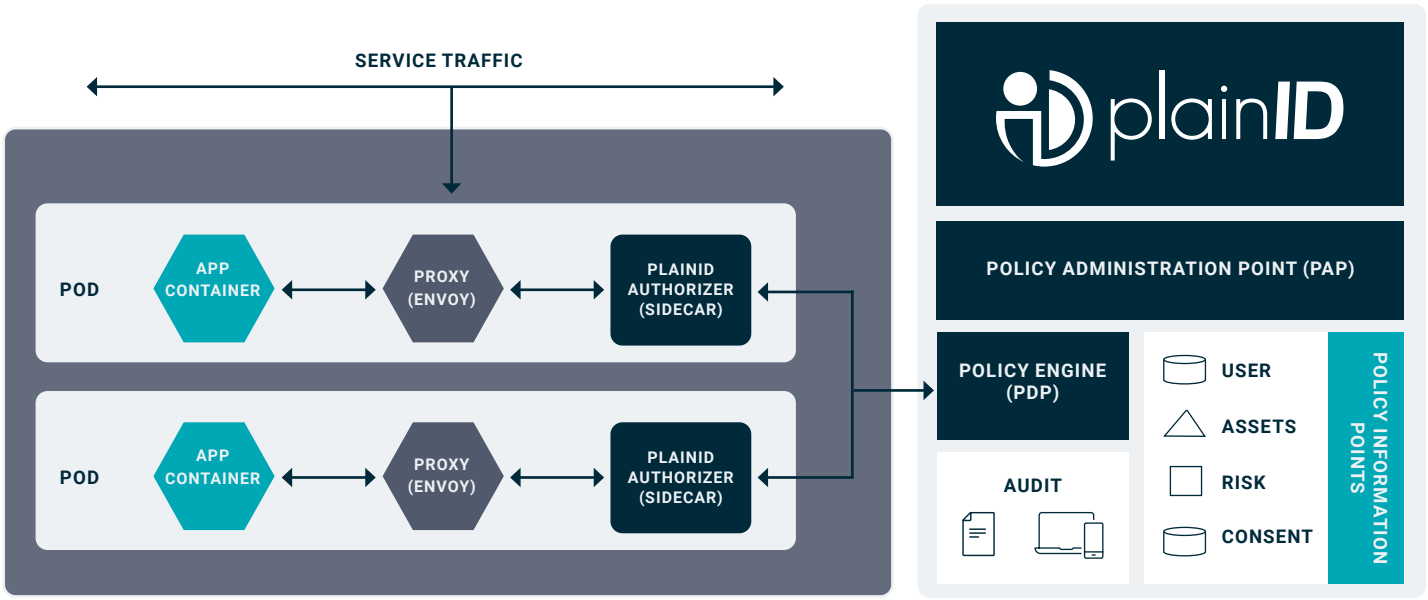


Authorization for Secure Microservices Architecture via Sidecars and Service Meshes

Integrating PlainID with a service mesh architecture for microservices can significantly enhance security and streamline policy enforcement.

Some examples of how PlainID provides authorization for microservices:

- **Sidecar Integration:** Each microservice can be equipped with a sidecar proxy that integrates with PlainID, ensuring all inter-service communications pass through dynamic authorization checks. This architecture centralizes security controls while maintaining service autonomy.
- **Service Mesh Integration:** By leveraging service meshes like Open Service Mesh in conjunction with PlainID, enterprises can implement a uniform policy enforcement layer across all microservices. This approach simplifies managing access control and securing communications in a distributed environment.



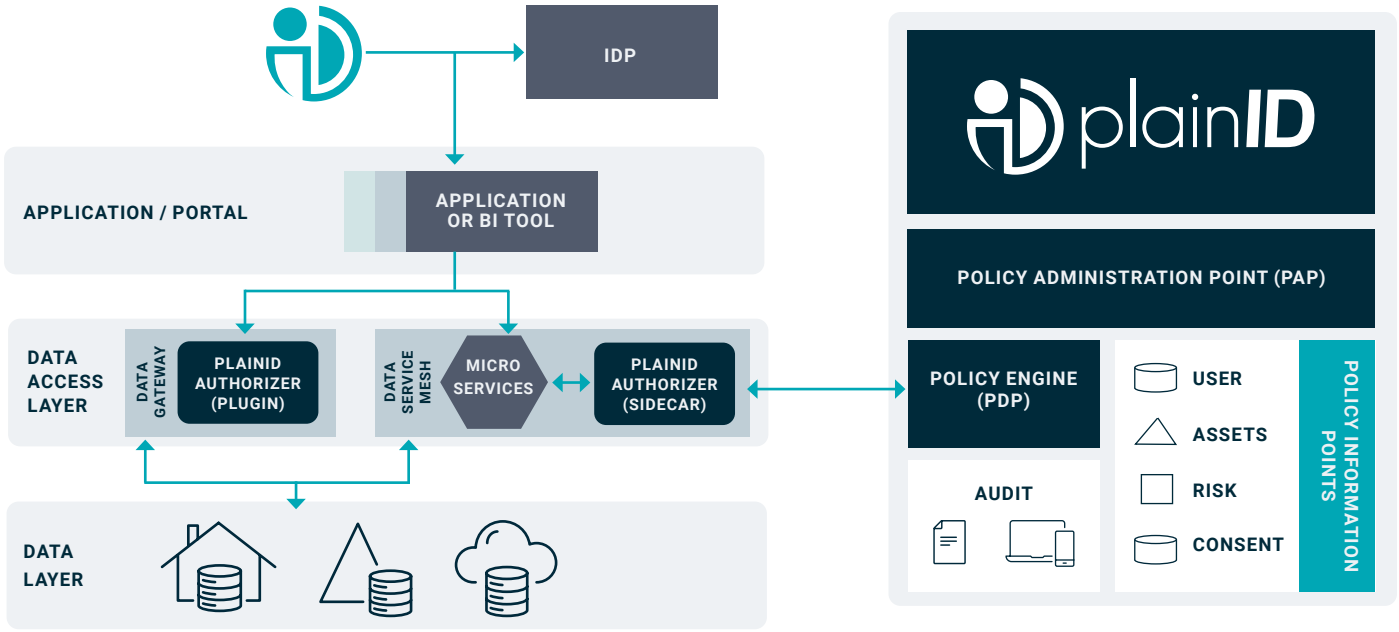
Data Layer Security Enhancement with PlainID

Securing access to data stored in data lakes or databases like Google BigQuery can be enhanced through PlainID's fine-grained access control capabilities.

Here are some examples of how PlainID addresses data access control:

- **Granular Access Control:** Implementing PlainID allows for the definition of detailed access policies that govern who can access specific datasets, tables, or even rows within a database or data lake, based on the user's role, purpose of access, and data sensitivity.
- **Dynamic Data Masking and Filtering:** PlainID can dynamically adjust the visibility of sensitive data based on the accessing user's attributes and context, thereby enhancing privacy and compliance with regulations without altering the underlying data structure.
- **Compliance and Auditing:** With centralized policy management, PlainID facilitates compliance with data protection regulations by ensuring only authorized access to sensitive data. It also provides auditing capabilities to track access and changes to data policies, helping enterprises maintain a comprehensive access log.

Leveraging PlainID's Dynamic Authorization Service enhances security in each layer of the technology stack by providing a centralized, dynamic, and context-aware mechanism for managing access across applications, APIs, microservices, and data layers. This approach not only secures digital assets but also aligns with modern agile development practices and cloud-based architectures, enabling businesses to adapt quickly to changing security requirements and scale securely.



Conclusion

In the rapidly evolving cybersecurity landscape, the need for robust and adaptable access control mechanisms is more pressing than ever. Traditional access control models like RBAC and ABAC have been foundational but increasingly fall short in addressing the complexities of modern digital environments. This is where Dynamic Authorization and Policy-Based Access Control (PBAC) come into play, offering a more nuanced, flexible, and context-aware approach to securing digital assets and user interactions.

The Importance of Dynamic Authorization and PBAC

Dynamic Authorization and PBAC stand out for their ability to make real-time access decisions based on a comprehensive evaluation of user context, the sensitivity of the data or resources being accessed, and current threat levels. This level of granularity and adaptability is essential in today's digital landscape, where threats are not only more frequent but also more sophisticated. By integrating these advanced access control mechanisms, enterprises can protect against unauthorized access and data breaches, which remain a significant threat, with unauthorized access accounting for a considerable percentage of all data breaches.

The Strategic Advantage of PlainID's Solutions

PlainID's Dynamic Authorization Service leverages these principles to offer a solution that is both powerful and user-friendly. By centralizing policy management and employing dynamic, real-time authorization decisions, PlainID helps enterprises navigate the complexities of access control with ease. The service's architecture, including its SDKs, API gateway integration, and focus on object-level security, provides a comprehensive framework that addresses specific OWASP concerns like broken object level authorization (BOLA). This strategic focus not only enhances security but also improves operational efficiency and compliance with regulatory standards.

PlainID's approach, focusing on protecting objects accessed through APIs rather than just the endpoints, offers a nuanced method of securing applications and data. This object-level attention ensures that even within broadly permitted access scopes, sensitive data or functions remain securely gated based on the dynamic context of each access request. Such precision in access control is critical for maintaining the integrity and confidentiality of digital assets in a landscape marked by sophisticated cyber threats.

Final Thoughts on Advanced Access Control in Securing Digital Transformation

As enterprises continue to embark on digital transformation initiatives, the role of advanced access control systems like those provided by PlainID becomes increasingly critical. These systems offer not just security but also enable the agility and innovation that come with digital transformation. By ensuring that access controls can dynamically adapt to new services, architectures, and compliance requirements, PlainID's solutions represent not just a defense mechanism but a strategic enabler of digital business.

The journey toward digital transformation is fraught with challenges, but with the right access control strategies in place, enterprises can pursue innovation with confidence, knowing their assets and users are protected. As we move forward, integrating Dynamic Authorization and PBAC into the cybersecurity framework will be paramount for enterprises aiming to thrive in the digital era, underscoring the indispensability of advanced access control in the foundational architecture of secure, digital enterprises

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.