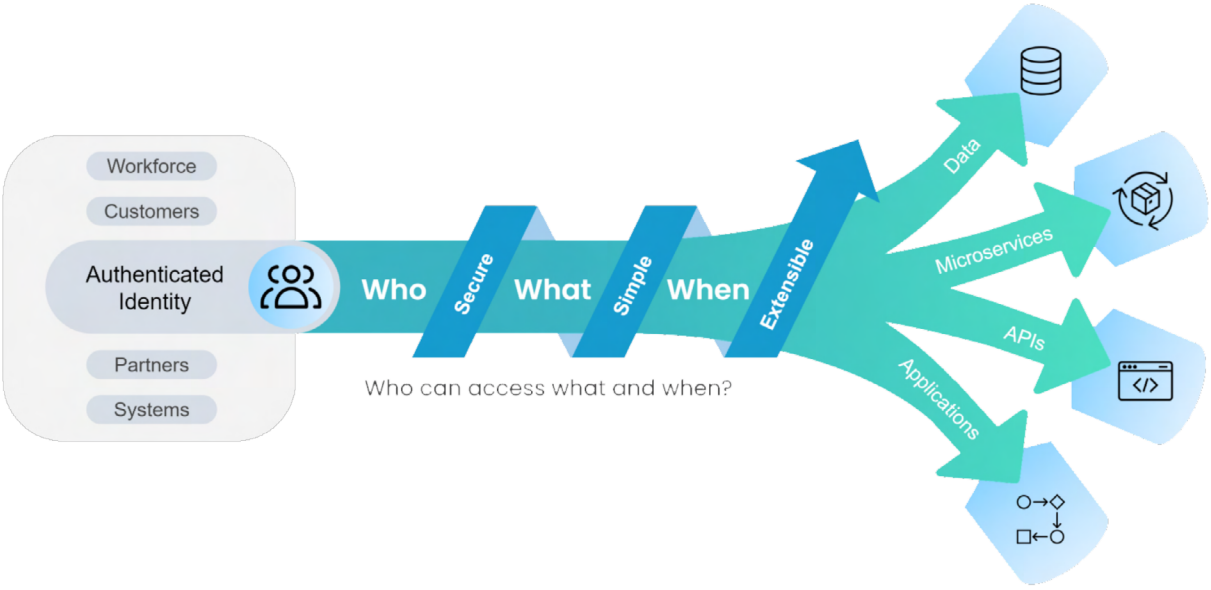
Enhancing Data Security with Externalized Authorization

Addressing the Impacts of Data Access Control for the Modern Enterprise

The Challenge of Connecting Identities to Data

Rapid digital transformation has fueled an explosion of data for many organizations. This growth brings with it significant challenges as organizations build initiatives to address security gaps in data access control.

Data, both operational and analytical, is critical for applications and business intelligence. However, vulnerable access points pose a data breach risk for organizations with sensitive data. As organizations continue to modernize their systems and applications, the ability to control who can access what and when has become more complex. Securing and facilitating the connections between the different types of identities (ie. workforce, customer, partners, third party, machine, etc) and data assets is both a business and a security imperative.



In this guide we explore the data access challenges enterprises face, the impacts it has on the business, security, and privacy, and what enterprises can do to improve their security posture and move at the speed of business.

Data Security Challenges of the Modern Enterprise

Managing data security is a major challenge that cuts across all industries and regions. Point solutions address it from various angles such as data encryption, data classification, data governance, and so forth. This tactical approach addresses the immediate needs of teams that own and directly interact with the data regularly (i.e. data teams, analytics, etc). However, it does not address the needs of security, identity, and architecture teams that need to manage data access control at an enterprise-wide level consistently. There are three primary challenges security, identity, and architecture teams face with data access control:

- The lack of central management for access control
- A diverse and distributed technology stack
- The complexity of identity and data

> "Security starts when authentication ends."
>
> Simon Moffatt, Founder & Research Analyst of The Cyber Hut

THE LACK OF CENTRAL MANAGEMENT FOR ACCESS CONTROL

Identity and Access Management have come a long way with standardization. It has taken decades for enterprises to adopt Single Sign-On (SSO) as the de facto for user authentication. Now that authentication is widely understood, enterprises are looking for ways to standardize authorization and better manage access control.

Applications are traditionally built with access policies embedded deep within application code. This causes business lines to have lengthy and inconsistent ways of implementing and managing authorization. Consequently, the lack of standardization causes headaches for security teams when it comes to auditing and managing policies for various business lines that are required to follow security protocols.

This causes a bottleneck when trying to keep up with changes in business decisions. Policy changes require application changes - application changes require coding, testing, and security reviews.

Security reviews are especially lengthy and cumbersome when there are islands of authorization siloed across applications. Each step forward into the new world spawns exponential amounts of work.

A DIVERSE AND DISTRIBUTED TECHNOLOGY STACK

Modern architecture has been monumental in supporting business agility. However, it also came with side effects. The move to cloud and hybrid architecture, as well as the rapid growth in data, APIs, and microservices brought on a new problem: exposed and vulnerable endpoints.

While these modern tools and solutions have their own native authorization capabilities they can only be engineered so far to meet unique business and security requirements. The ever-growing portfolio of technology (e.g. API gateways, service mesh, data gateways, data lakes, data virtualization, etc) makes it difficult for security teams to normalize authorization for all architecture layers. This causes companies to either compromise on security or slow down the business in order to maintain security.

THE COMPLEXITY OF IDENTITY AND DATA

Enterprises are faced with multiple types of identity that need access to specific data. Workforce identities need adequate permissions to resources for optimal productivity. This is especially relevant for data and business analysts, and unauthorized users, who might inadvertently have over privileged access to sensitive data.

Partner and third-party identities (e.g. contractors, distributors, suppliers, etc) also require a certain level of access to support various business lines. Similarly, customer-facing enterprises have end users that require access to relevant data to maintain a level of user satisfaction. In addition to user identities, how identities of machines, systems, and services interact with data needs to be accounted for when it comes to the enterprises' security posture. Traditional Data Governance solutions alone do not have the ability to fully utilize the power of a strong identity program - making it difficult for enterprises to implement identity-first and Zero Trust architectures.

All enterprises face data access control challenges that adversely impact security and revenue.

3 Key Business Impacts of Poor Data Access Control

Enterprises experience various effects of poor access control and it typically falls into three areas: security, operations, and time-to-market.

1 MAJOR GAPS IN SECURITY AND ZERO TRUST

The lack of visibility and control of who has access to what and when is one of the biggest pain points security and identity teams face. The growing number of users, applications, and data creates an immeasurable attack surface. Vulnerabilities span across architecture layers from applications, APIs, microservices, and the database - down to the very rows and columns where all data resides.

Solutions that attempt to address Zero Trust have generally focused on network security and more recently, authentication. These solutions are not enough because the “last mile” of the digital journey remains unprotected wherever access policies are poorly or not consistently implemented. Access controls via traditional solutions are unable to provide the necessary identity-aware context in real-time (i.e. runtime authorization) that is paramount for the dynamic fine-grained authorization that is required to properly secure the enterprise.

In many cases, enterprises use data views as a means to present a subset of the data to limit its exposure. This tends to complicate the situation further for security teams. Creating hundreds and thousands of permutations of data explodes the number of assets that need protection. Typically static roles and attributes internal to the database itself are used as an attempt to close this gap, but this leaves out the ability for dynamic authorization - it does not harness the full power of identity and its context.

Data access control becomes even more critical for continuous security where risk signals need to be considered in real time to best protect highly sensitive data for security, privacy, and regulatory compliance (e.g. GDPR, CCPA, CPPA, HIPAA, etc).

> “Security and risk management technical professionals should mitigate digital access risk by modernizing runtime authorization controls.”
>
> Homan Farahmand, VP Analyst and GTP Advisor at Gartner

2 HIGH OPERATING COSTS & COMPLEXITY

Embedding unique authorization codes into applications and data tools is a bandaid to a larger security problem. While taking the "do-it-yourself' (i.e. homegrown) approach has some immediate benefits and may appeal to development teams, the associated costs have long-term effects. Homegrown approaches lack industry best practices. They provide no enterprise-wide framework for policy authoring, management, testing and approval workflows which negatively impacts efficiency and productivity.

Siloed data access control is dependent on highly technical and skilled expertise (e.g. architects and developers) to alter code, write policies and understand application-specific logic for access control. These personnel costs could be diverted to tasks and feature development towards generating business value within the application supply chain.

Layers of APIs, microservices, and multiple types of databases create unique requirements. Maintaining interoperability is resource intensive when different solutions are often incapable of speaking the same language. Legacy and homegrown access control typically requires technical expertise for maintenance amounting to lengthy processes and overhead.

This leaves out the business team and non-technical users entirely as access control code becomes a black box of classes and methods instead of being based on plain language that anyone can understand. As the environment becomes undoubtedly complex overtime, it is resource-intensive to manually ensure data access is normalized across endpoints.

3 SLOW TIME-TO-MARKET & FRUSTRATING USER EXPERIENCES

Business and development teams are pressured to accelerate time-to-market and its value. This is more critical when revenue is tied to data productization and data monetization projects. Without comprehensive data access control, security teams are unable to simultaneously enforce security requirements and accelerate business initiatives.

Business and development teams are pressured to accelerate time-to-market and its value. This is more critical when revenue is tied to data productization and data monetization projects. Without comprehensive data access control, security teams are unable to simultaneously enforce security requirements and accelerate business initiatives.

Business and development teams lack reusable building blocks for data access control to accelerate secure and compliant application rollout. This hinders the repeatability of business processes. It also minimizes the enterprise's ability to respond to changes in business decisions and future growth.

Lastly, poor authorization impacts productivity and user satisfaction for workforces and customers, respectively. For example, customers and employees expect a frictionless experience whether it's making a banking transaction or attempting to make changes to their customer profile. Dissatisfied users are ready to move on to competing products and services which eventually impacts revenue growth over time.

3 Key Benefits of Enhancing Data Security through Externalized Authorization

Enterprises have unique requirements shaped by the current state of their infrastructure and pending roadmap items. However, a common goal shared across all enterprises is maintaining data security across architecture layers (i.e. API gateway, service mesh, databases, etc) - down to the data asset itself.

By externalizing authorization, enterprises benefit from a unified approach that meets requirements prescribed by security, architecture, business and data teams. This approach provides centralized management for tighter control of data access, lowers operational costs, grants visibility into security across the stack, and accelerates time-to-value.

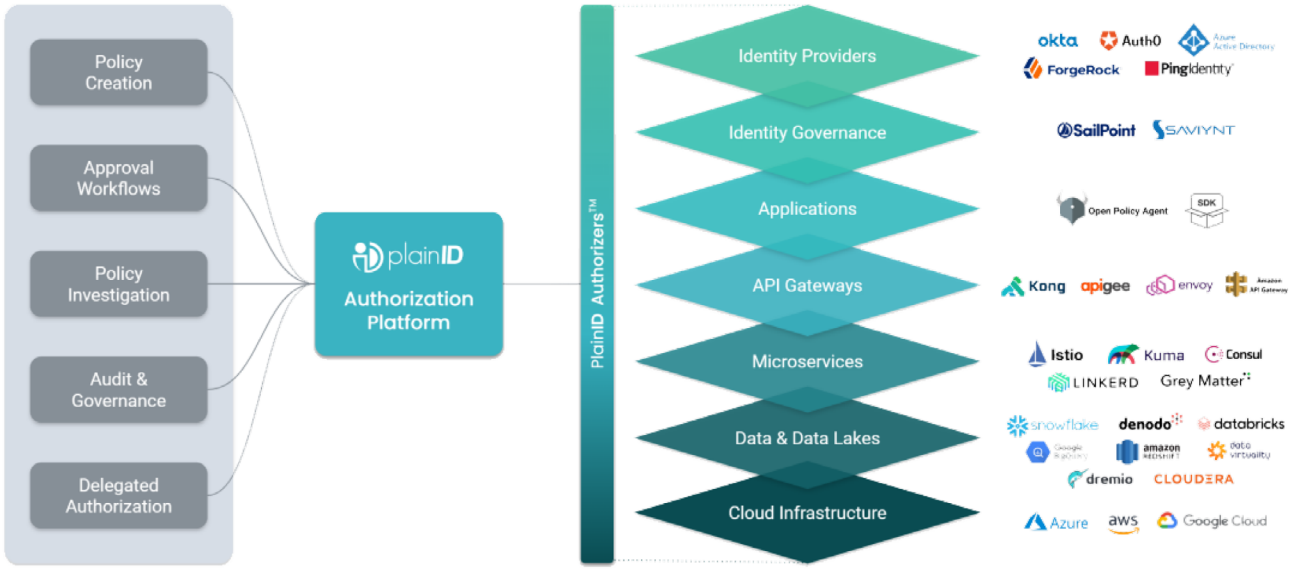
1 MAXIMIZE CONTROL AND VISIBILITY OF DATA ACCESS WITH CENTRALIZED MANAGEMENT

Zero Trust frameworks require access policies to be based on real-time context to continuously block unauthorized access and lateral movement throughout an environment. Externalized authorization, and its centralized management, enables enterprises to map and visualize complex relationships between identities and data. Traditional approaches that embed access policies inside applications are static and incapable of addressing identity-aware security.

Identity-aware security has major implications for compliance and data privacy. Dynamic authorization's ability to fine-tune access to various types of data (and its granularity) for authorized users and services contributes towards stronger data stewardship and addresses the compliance requirements mandated by regional regulatory bodies. Centralized management of authorization policies simplifies and enhances enterprise-level access control for stakeholders such as security, identity, compliance, business, developers, and data teams.

What is Dynamic Authorization?

Dynamic Authorization is access control that gathers information from multiple identity and data sources in real-time to accurately determine what data or resource a user or machine has access to. It also includes the functions (i.e. create, read, update, delete) that they are allowed to perform once they access an application, system, service, data, or other asset.



Digital identities are rich in contextual information, but passing all of this information on in a single token is not possible.

Capabilities such as token exchange and token enrichment powered by policy-based access control are key to making sure the right information is available at the right time for the right resources no matter how fine-grained. This is invaluable for data security as identities move through architecture layers of APIs, and microservices to access data. For example, when a user requests access to sensitive data, the data can now be filtered and masked at the column, row, and cell level, based on the identity's context and risk signals in real-time.

2 LOWER OPERATIONAL COSTS & REDUCE COMPLEXITY

Enterprise architecture has become more complex. Siloed authorization tucked away in various third-party and homegrown solutions exacerbate the complexity - making it harder and costly for enterprises to control data access.

Centralized management, powered by policy-based access control (PBAC), provides a business-driven approach

What is Policy-based Access Control (PBAC)?

Policy-based Access Control is a comprehensive authorization approach that uses both attributes and roles to determine access decisions. PBAC goes beyond static approaches such as Attribute-Based Access Control (ABAC) and Role-based Access Control (RBAC) and simplifies how enterprises manage access through policy authoring through plain language that makes it easy for non-technical stakeholders to create, manage and enforce policies.

that empowers business and security managers, as well as data teams. Non-technical users can leverage PBAC for its capability to quickly design authorization policies using plain language. Less training is required for business and application owners who are responsible for maintaining the right level of access to their applications and services.

As dependency on Policy-as-Code (PaC) methods such as Open Policy Agent (OPA) grows in popularity among developers, it's becoming increasingly important to have a centralized policy management approach that makes it easier for various teams to manage how users access data specific to their projects and lines of business.

Centralized management simplifies access control for enterprises with complex architecture. Enterprises can reduce operational costs and future-proof access control through a unified and extensible approach that addresses data security and other use cases (e.g. external-facing portals, legacy migration, deployment patterns, etc.).

3 ACCELERATE TIME TO VALUE & IMPROVE USER SATISFACTION

Whether access to data is needed for external-facing applications or internal business optimization projects (e.g. business intelligence and analytics) - the ability to move quickly and securely at the speed of business is critical for revenue generation. Using data as a business engine through data productization and data monetization has become increasingly important for lines of revenue. It's equally important to carry out these projects without compromising security.

Various teams such as business managers and data scientists need quick access to data to build new products and services. Centralized management and PBAC provide essential authorization capabilities to secure connections between identities and data.

Externalizing access controls enable enterprises to standardize and provide repeatable building blocks for business and development teams. Distributed enforcement to specific data technologies via Authorizers, alongside central management, gives security teams enterprise-wide visibility and control of data access.

What is an Authorizer?

An Authorizer is a pre-built integration for third-party solutions that provide access control for vital authorization enforcement patterns such as API gateways, microservices, data lakes.

Authorizers extend centralized management of access control to targeted data solutions including: Snowflake, Denodo, Dremio, Trino, Google BigQuery, Istio, Apigee, AWS API Gateway, and many more.

Distributed enforcement for specific databases, data lakes, and data virtualization layers through Authorizers accelerates time-to-value for various teams that rely on different sources for their data projects. Allowing organizations the fastest path to bring the full power of identity to the data layer. This means data can be shared and exposed securely, giving the right people the right amount of access.

In the context of workforce users, data filtering and masking can be applied to expose data specific to their project or responsibility.

For example, a local bank teller should not be able to see a customer's social security number. Or a local bank branch teller may not be authorized to see the account details of high-net-worth individuals. Similarly, enabling customer users to view and edit non-sensitive information can eliminate friction and improve their user experience. Changes in conditions and risk signals can prompt necessary friction where sensitive transactions occur (e.g. moving a high dollar amount, accessing sensitive health records, etc). Delivering frictionless experiences impacts business profitability. Having the right access controls in place impacts both workforce productivity and customer satisfaction.

Similarly, enabling customer users to view and edit non-sensitive information can eliminate friction and improve their user experience. Changes in conditions and risk signals can prompt necessary friction where sensitive transactions occur (e.g. moving a high dollar amount, accessing sensitive health records, etc). Delivering frictionless experiences impacts business profitability. Having the right access controls in place impacts both workforce productivity and customer satisfaction.

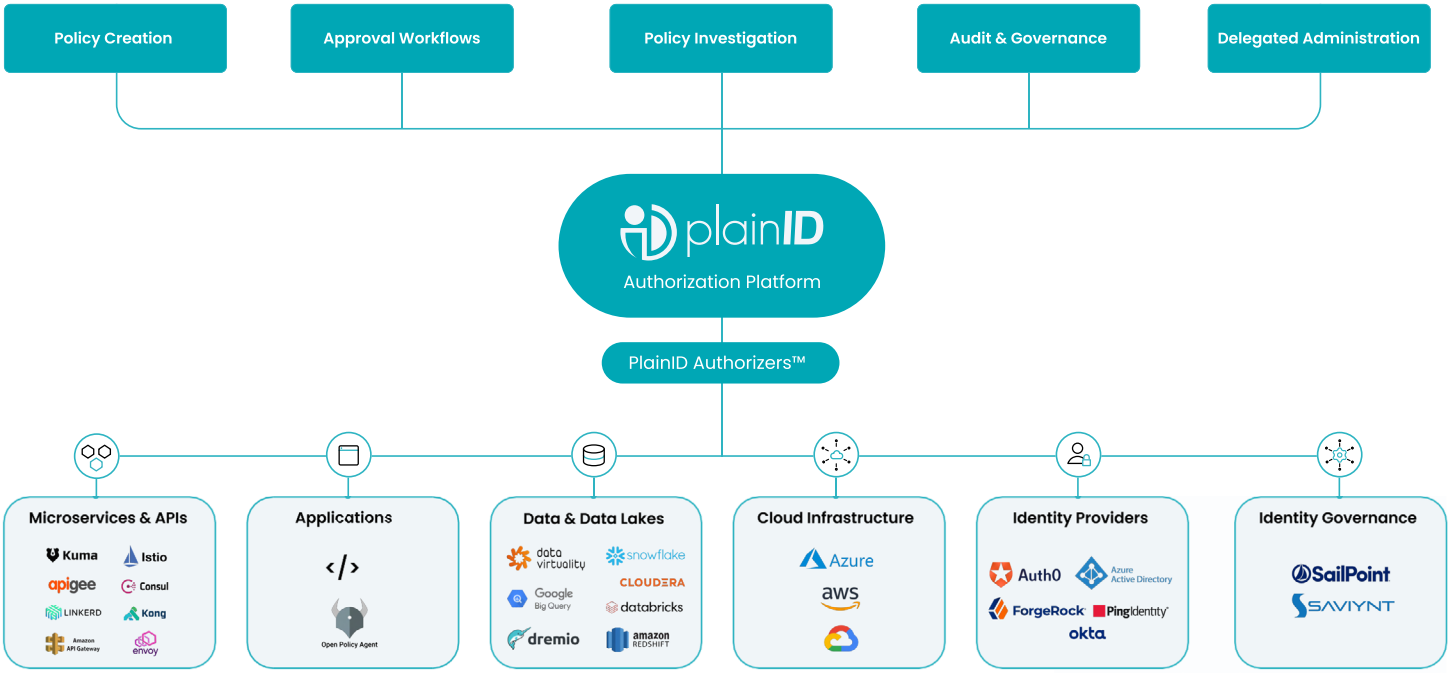
KEY TAKEAWAY

The benefits of externalizing management are realized by enterprises of all sizes and industries. Centralized management of access control bolsters enterprise-wide data security, lowers operational costs and complexity, and accelerates time-to-market and its corresponding value for revenue generation.

The PlainID Authorization Platform

The PlainID Authorization Platform™ is designed to securely manage the connection between digital identities and assets across the enterprise. The Platform simplifies management with its Policy-Based Access Control (PBAC) framework which allows you to create, manage, and enforce Dynamic Authorization in a business-driven and user-friendly way in plain language. It also provides the necessary controls and insight into the entire user journey to data in real-time.

Centralized Management with Distributed Enforcement

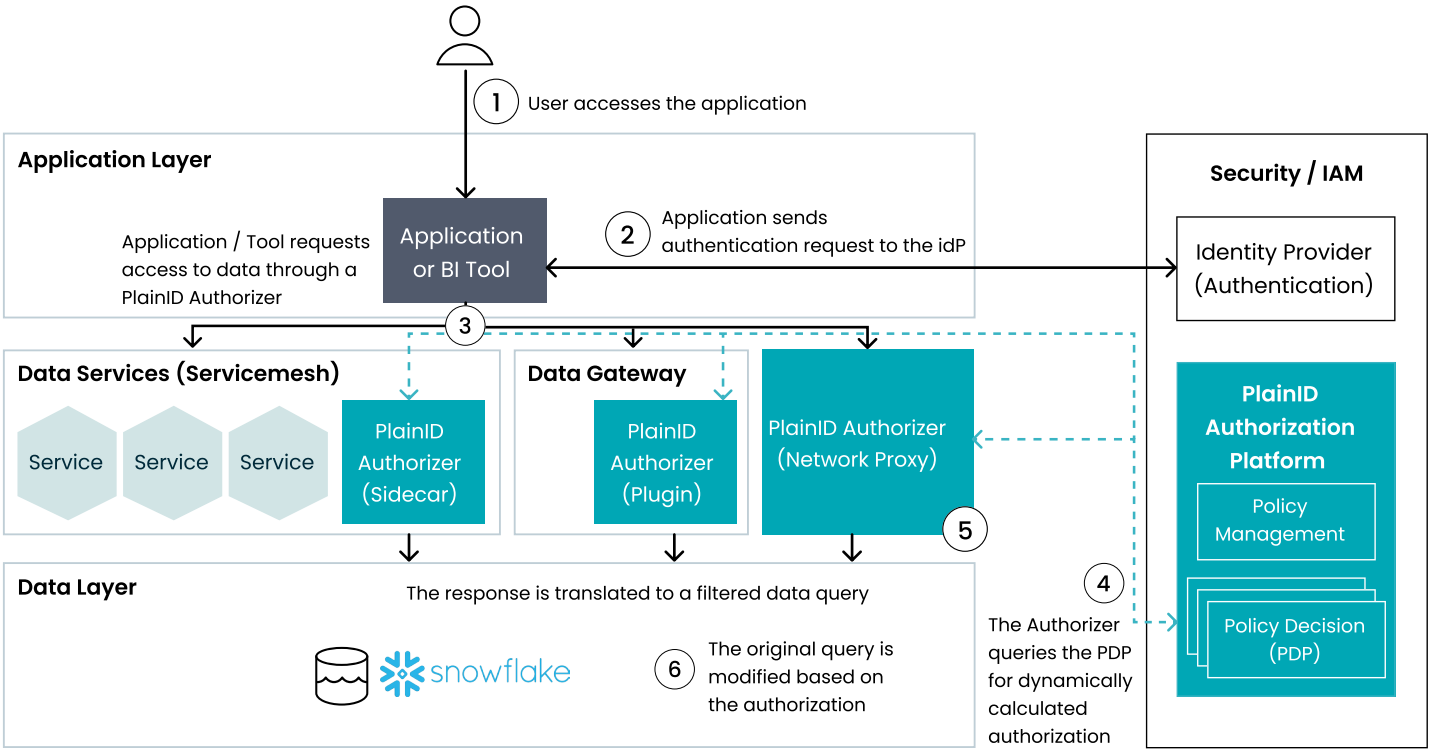


PlainID Authorizers™, out-of-the-box integrations, provide extensible Authorization modules for distributed enforcement across your technology stack authorization patterns. Authorizers are available for microservices, APIs, and data lake tools such as Istio, Apigee, and Snowflake, respectively.

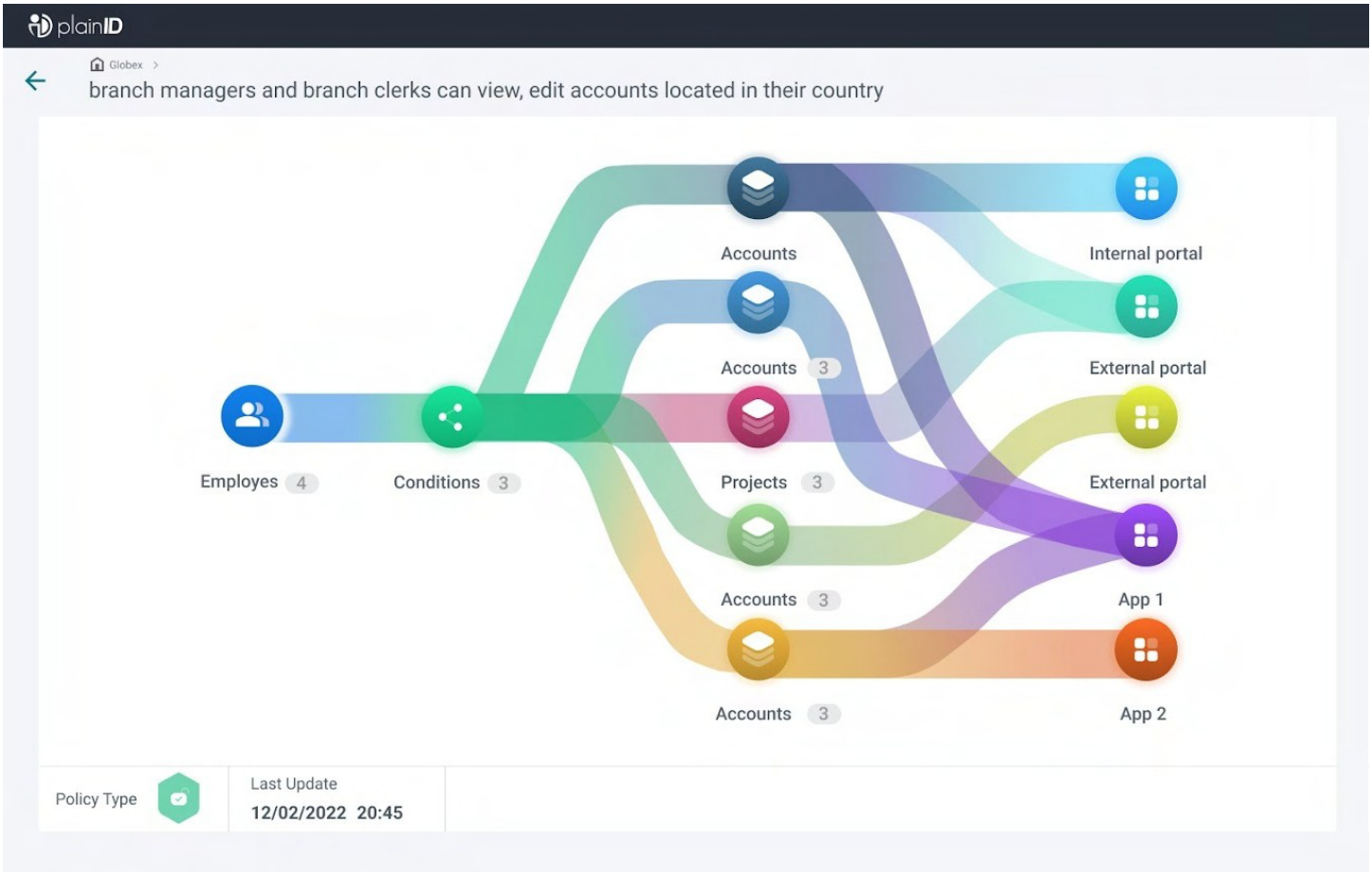
Authorizers protect data (e.g. data filtering, data masking) throughout the stack in a variety and interface with the existing systems as a:

- Plugin
- Network proxy
- Sidecar (for a service mesh)

Plugins are installed on data infrastructure, and network proxies sit in front of data mediums and manipulate the queries that are passed to it based on identity and contextual information in the policy. Data manipulation (e.g. update, create) can be controlled via Authorizers in the service mesh, as well as plugins that exist directly in the data store. PlainID Authorizers also have the ability to control policy that is internal to data platforms that do not support either plugins, management such as policy creation, approval, testing and governance when access control decisions can not be externalized.



The Platform is designed to help enterprises adopt authorization policies at scale by making it easy for stakeholders to create, manage and enforce policies. The platform also improves policy workflows and time-to-market for applications by providing tools to visualize and test policies before going live.



Go beyond traditional authorization solutions by modernizing workflow processes for all enterprise stakeholders. The PlainID Authorization Platform mitigates security risks while simultaneously making your business more agile.

Get a demo and learn more about how PlainID can improve data security for your enterprise.

GET A DEMO