Integration for a Resilient Data Protection Framework

Gain complete visibility and control of enterprise data

Protecting data assets consistently across various databases poses a substantial challenge for data owners. The intricate web of permissions often obscures transparency, making it difficult to manage access effectively. Many repositories lack fine-grained access controls, neglecting the full scope of user identities, risk signals, and data classification from other security tools. Authorization plays a critical role in solving data protection challenges by providing a structured and controlled approach to managing access to data.

Organizations that fail to have a robust and forward thinking data protection strategy are exposed to a wide range of risks, including financial and legal consequences; reputational damage and operational disruptions.

Customers use BigID to reduce their data risk, automate security and privacy controls, achieve compliance, and understand their data across their entire data landscape: including multi-cloud, hybrid cloud, IaaS, PaaS, SaaS, and on-prem data sources. BigID allows organizations to discover, manage, protect and get more value from their regulated, sensitive and personal data across the enterprise.

PlainID offers a forward-thinking approach to Authorization, empowering businesses with the latest and most advanced technologies to address the unique requirements of the Enterprise. PlainID provides a platform that centralizes the management and control of authorization policies across the enterprise technology stack.

Key Benefits of the Integration

- Apply consistent data security categorization and labels at all levels through Policy-Based Access Control
- Enhance security with Dynamic Real-Time, Context-Based Access Decisions
- Accelerate time-to-data while also applying enterprise wide security controls based on Data Governance
- Minimize security gaps by centralizing data access control and data governance solutions
- Enhance visibility and control of access policies and improve Data Governance audits

PlainID and BigID together strengthen data protection

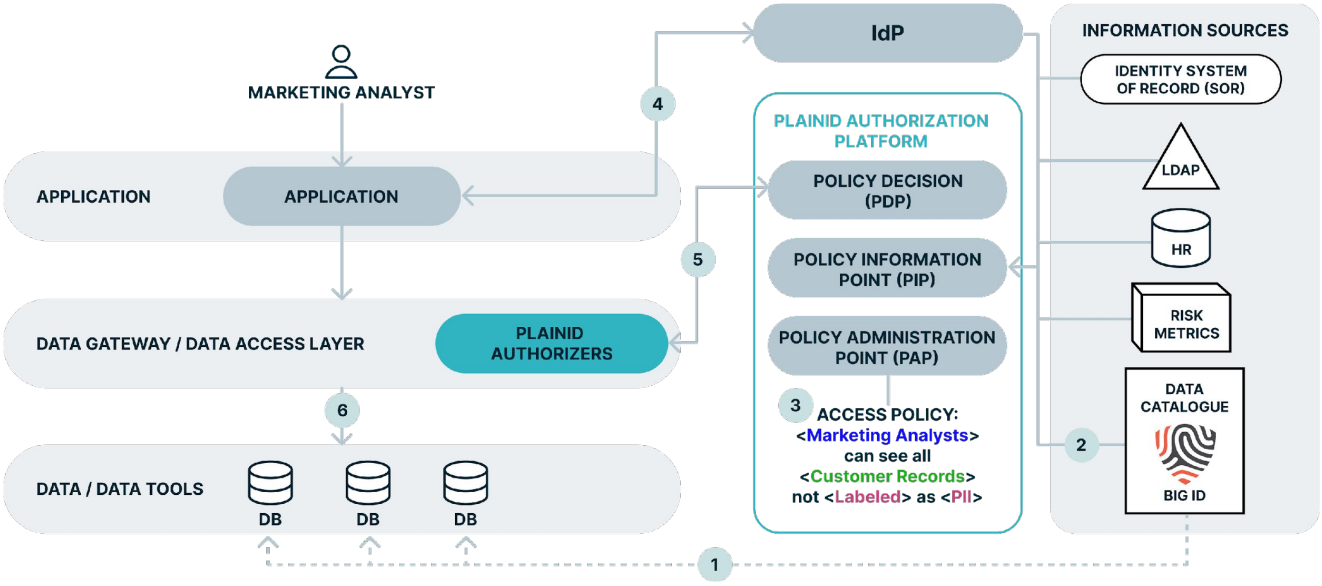
By combining solutions from PlainID and BigID, enterprises gain complete visibility and control of their data. Together, the solutions allow organizations to

- Consistently protect data no matter which form it takes, JSON, SQL, Language Objects
- Provide closed loop remediations for issues found by BigID Data Security Posture Management
- Close up gaps detected by overexposed user access in BigID

The integration of PlainID's Authorization Platform with BigID creates a powerful combination that allows companies to ensure their sensitive and personal data will be protected.

This integrated approach enables organizations to maintain consistent policy-based access control across the entire technology stack, leading to enhanced security, increased user productivity, and reduced administration mistakes.

Combined Solution Use Case



- BigID discovers and classifies data across the different databases.
- BigID's data classification is integrated into PlainID's Policy Information Point (PIP) as a source of attributes for data-type assets, enabling their utilization in the configuration of access policies and access decision calculation.
- A policy is configured within PlainID's Authorization Platform to deny <Marketing Analysts> access to <PII>. In this policy, the information about a user indicating they are a <Marketing Analyst> can be retrieved from the IdP, LDAP, HR system or an identity SOR such as IGA. <Customer Records> is the data asset configured within the PlainID's PAP. BigID provides information about which columns are <Labeled> as <PII>.
- The data access request is evaluated at runtime when a user attempts to access records, and a access decision is dynamically calculated. Using the PlainID PIP service, the information about which columns are <Labeled> as <PII> is pulled in real time from BigID to modify the original query. In this example, the SELECT clause will be modified to exclude / mask the columns containing <PII>. The technical mechanism of modifying the query is contingent on the architecture access pattern.
- The <Marketing Analysts> can access the sales and marketing reports excluding <PII> or with masked <PII> columns.

Takeaway

PlainID specializes in creating, managing, and enforcing access policies, while BigID focuses on the discovery, labeling, categorization, and security assessment of data. By integrating these two powerful tools, organizations can ensure that their data is accessed only for intended purposes and in appropriate ways. This leads to consistency, visibility, and a standardized approach to data protection across the entire enterprise.

ABOUT PLAINID

PlainID is The Identity Security Company™. We help identity-centric enterprises defend themselves from adversaries who use identity-based attacks. Our Identity Security Posture Management Platform provides Identity Insights, SaaS Authorization Management, and Dynamic Authorization Services to create identity-centric security across SaaS, APIs, microservices, apps, and data powered by policy-based access control. Visit PlainID.com for more information.