

Financial Market Infrastructure Company Streamlines Workforce Access with Policy-Based Access Control

A leading post-trade market infrastructure provider embarked on a journey to modernize its access control systems. As it transitioned from static role-based access to a dynamic, scalable model, the organization faced challenges managing workforce access across various platforms. To address these challenges, the company adopted PBAC to centralize and streamline its authorization processes, improving security, reducing operational overhead, and increasing flexibility in its access controls.

CHALLENGES

- **Static, Role-based Controls for Data Access:** Access control systems that were largely static and role-based led to over-provisioning, causing operational inefficiencies and security risks.
- **Administrative Overhead:** Manual management of access requests and recertification processes increased compliance and operational burden, as reviews of access privileges had to be validated regularly.
- **Unsecure, Permanent Access for the Employees:** Permanent access was often granted without sufficient contextual validation, leading to increased risk exposure.
- **Siloed Management of Access Controls:** Separate teams managed access for workforce and clients, which added to the complexity of standardizing access management practices across the organization.

As we modernized our enterprise architecture, it became clear that our legacy access control systems were limiting scalability and flexibility. By leveraging Policy-based Access Control, we were able to align authorization with our architecture's dynamic needs, ensuring secure, adaptable, and efficient management of our infrastructure.

Identity & Access Management Director



INDUSTRY: Financial Services

EMPLOYEES: 5,000+

LOCATION/HQ: New York, NY USA

CHALLENGES

- Data Access Without Dynamic Control
- Administrative Overhead
- Over-privileged Access to Data
- Siloed Management of Access Controls

SOLUTION

By implementing Policy-Based Access Control (PBAC), the organization transitioned from static, role-based access to a more dynamic and flexible model. This shift enabled the company to adjust access based on context, streamlining its access control processes and enhancing both security and operational efficiency.

SOLUTION

PlainID was chosen to address these challenges and streamline their identity and access management (IAM) system. By implementing PBAC, the organization moved towards a more dynamic and flexible access management model that replaced static role-based controls with policies that could adjust access based on context and risk.

Key Features and Implementation Highlights:

- **Centralized Access Control for Workforce IAM:** The PlainID solution centralized access management across multiple teams, enabling consistent and efficient access control for workforce-related systems.
- **Integration with On-premises and Cloud Systems:** PlainID supported the organization's legacy systems, such as Oracle and PostgreSQL, while also integrating with modern data platforms.
- **Dynamic, Fine-grained Authorization for Databases:** PlainID is used to control access to databases. Users request access through a self-service portal, where the system checks identity-based context in real-time and access is granted or denied based policies – giving users temporary, secure access when needed.
- **Extensive Coverage for Enterprise Technology Stack:** The PlainID Platform future-proofs their architecture by focusing on improving access control for data-rich environments such as Snowflake and Power BI. The organization aims to achieve even greater scalability in workforce access management, while further reducing operational risk.

BUSINESS RESULTS WITH PLAINID



IMPROVED SECURITY & COMPLIANCE

Enhanced Security Posture: By shifting from static roles to dynamic, context-aware access controls, the organization was able to improve its security posture, reducing the risk of over-provisioning and unauthorized access.



OPERATIONAL EFFICIENCY

Reduced Developer Overhead: PlainID significantly reduced the manual effort required for managing access controls, saving administrative time and allowing administrators and IAM managers to focus on higher-value activities.



SCALABILITY & FLEXIBILITY

Support for Enterprise Ecosystem: As the organization continues to expand, the scalable nature of PlainID's solution ensures that their workforce IAM system can easily adapt to new platforms and evolving business requirements.

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. Visit PlainID.com for more information..