Evaluating Authorization Vendors

Supported by The Cyber Hut

plainID

Vendor Evaluation

Identity and Access Management can be a complex topic and one area where this complexity is most evident is in access control. Evaluating an authorization provider requires a range of steps that can help remove the information barriers between the buyer and the provider.

Reduced Business Friction

A key issue many CISOs face is knowing how to allocate finite resources — such as people, license spend and effort — and how to do so against an ever-growing list of security threats. However, this battle needs to be completed under the continuous eye of the business — where security controls that are too inhibitive or introduce and amplify friction will not only be unacceptable but often avoided by end users if they are implemented.

BUSINESS OUTCOME	DELIVERED BY
Improved Employee Onboarding	**Reusable Policy-Based Access** — By allocating users with the correct access when they join an organization, the speed at which they can start working is greatly expedited. The use of modular policies to allocate access (often incorporating RBAC, ABAC and contextual information) supports this approach.
Optimized Team Working	**Improved Line of Business Access Management** — By providing non-technical line of business managers with the ability to perform permission management (users to objects) or be part of the policy design process means the right staff members get the right access they need.
Optimized Hybrid Working	**Improved Intra-Team Data Sharing** — Data collaboration is a key component of a modern enterprise's ability to solve complex problems in an agile and timely fashion. The ability to share to other teams (even from other organizations) can be designed using dynamic policy-based access control that contains identity data, context and a broad array of data assets.

What Capabilities Should the Vendor Provide?

CAPABILITY	DESCRIPTION
Platform Approach	A platform-wide set of capabilities that are specific to access control life cycle management — from the creation of controls, their enforcement and the governance surrounding them. This platform should be centrally managed and accessible by a range of different stakeholders interested in the protection of applications, APIs and data.
Policy Management	Authorization controls should be wrapped in a policy-based approach that results in reusable components which can be applied to a variety of different user communities, assets and stakeholders.
Policy Design	Policy design should be able to use a range of different data sources, including existing persistent identity stores, directories and databases, and more contextually aware signals such as risk, threat, device and location data. Policy creation should be both programmatic and by natural language user interfaces.
Enforcement	The enforcement of policy will be a critical component of the access control life cycle. A range of enforcement options will be needed, from inline proxies to microservice-based decision engines to APIs and SDKs to accelerate enforcement coverage.
Deployment Acceleration	Authorization is a key pain point for data, API and application access. The ability to deploy access control services and create and manage policy must be automated as much as possible, through a range of integration and management options.

Questions to Consider During Vendor Evaluation

CAPABILITY	EXAMPLE QUESTIONS
Platform Approach	1. Does the solution support a wide range of authorization capabilities? 2. Does the solution provide a centralized management console? 3. Is the management console designed to be used by a range of stakeholders, including non-technical line of business managers and application owners? 4. Can the platform be extended and customized? 5. Can the management console be delivered in a cloud environment? (either as a service or cloud-native private setting) 6. Can the authorization capabilities be made external from the application, API or data object being protected? 7. Does the platform support a range of standards-based integration options? (e.g., OIDC, OAuth2, LDAP, SCIM) 8. How does the platform help support a range of security architectures such as zero trust, identity-centric design and continual/adaptive risk? 9. Does the platform provide the ability to see who has access to what and why? 10. Does the platform support the ability to search for user permissions? 11. Does the platform support the ability to search for identity/subjects associated with a particular object/asset?
Policy Management	1. Can access control logic be encapsulated in policies? 2. Can policies be labeled, named, tagged and version-controlled? 3. Can policies be assigned to an owner? 4. Can policies be approved or tested before use against a production system? 5. Can policies be reused against a variety of user communities or target systems? 6. Can polices be duplicated or part-copied? 7. Can a policy be created programmatically? (e.g., REST API) 8. Can existing access control data be migrated into a policy framework? 9. Can policies be searched and queried?

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.