plainID
THE AUTHORIZATION COMPANY

SUMMARY BRIEF

Policy Manager offers a focused solution for Authorization management and control.
Simplified, Adaptive, Dynamic and Secure

Authorization

Authorization (AuthZ) is part of a larger area, commonly called – Identity and Access Management (IAM). IAM covers three different topics: Identity, Authentication and Authorization.

Identity

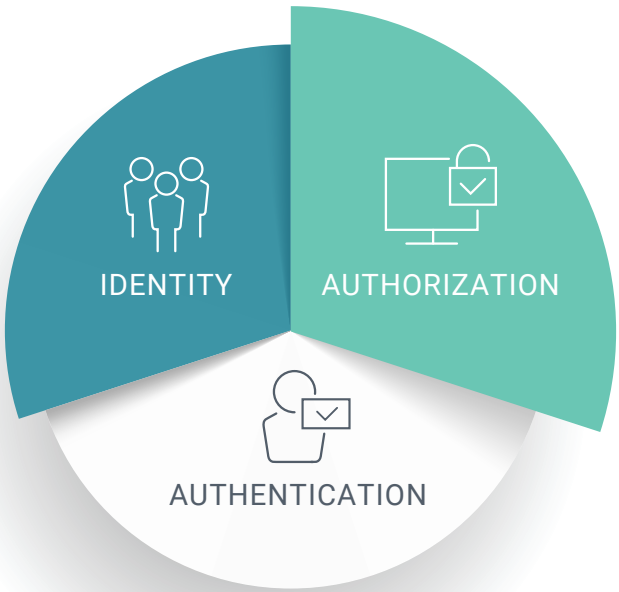
Specifies who the users are, their characteristics, attributes and so on. For example: Joe is a Sales Manager, working in region A. Identity mechanisms typically handle the lifecycle management of users, including on-boarding, role-changing and off-boarding.

Authentication (AuthN)

Verifies the identity, and continues to do so for the duration of the session. For example: Joe has provided an ID and password or fingerprint, so the system can clearly confirm his identity.

Authorization (AuthZ)

Dictates what the user is allowed or restricted from doing. Access is a part of AuthZ that relates to the ability to use an application or a service. For example: Joe can only view and manage accounts in his region. Access covers high level authorization (sometimes referred to as coarse-grained). For example: Joe can access the CRM and the ERP (but this access decision does not dictate what Joe can do in the CRM or ERP).



IAM Landscape

Authorization Solution Features

Authorization Solutions should address:

Business Orientation

Authorizations are inherently business-oriented, and the business owner of the data/resource is the person responsible for determining who is authorized to use it. For example: only the Human Resource Manager, who is responsible for the employees' data, can determine who can access which employees, and what extent of data will be viewed.

BUT… Authorization Management today is very technical, not user-friendly, and is typically managed by an IT department or people with specialized skill sets. Business owners cannot see and/or manage the authorization process, even though it falls within the domain of their responsibility.

Visibility

Authorization should be visible at all times for the organization. Answering the questions "Who can do what?" and "Who can use what?" should be easily possible whenever needed. Another level of this ability is answering: "Who has used or done what and when?"

THEREFORE…There is a high demand in most organizations for these answers, but this requires a lot of investigation, many hours of technical employee involvement, and alas, often all the questions are not answered.

Simplicity and Agility

Managing and enforcing authorizations for a new app, platform or system should be very easy and fast. There are so many changes in an average enterprise, that if it's not simple enough, then it just won't happen (according to statistics, an average enterprise implements around 40 new apps/system a year, and that doesn't even count the rapid migration to the cloud we see as well).

RESULT…The lack of simplicity in Authorization Management and control led organizations to employ large groups of "authorization managers" that manually update the Authorization in the applications and systems.

Modernization

Organizations' traditional boundaries are falling, and most have already moved or are talking about moving to the cloud, and implementing more mobile based solutions. In addition, there is a change in the on-premise technology, either by adopting private/public cloud or other more advanced technologies. The Authorization technology in those platforms also changed, what was once good for the legacy solutions doesn't always work that well now. The Authorization solution should support the movement from a repository-based to virtual token-based, from static to dynamic, so it can address the modernization of the data center.

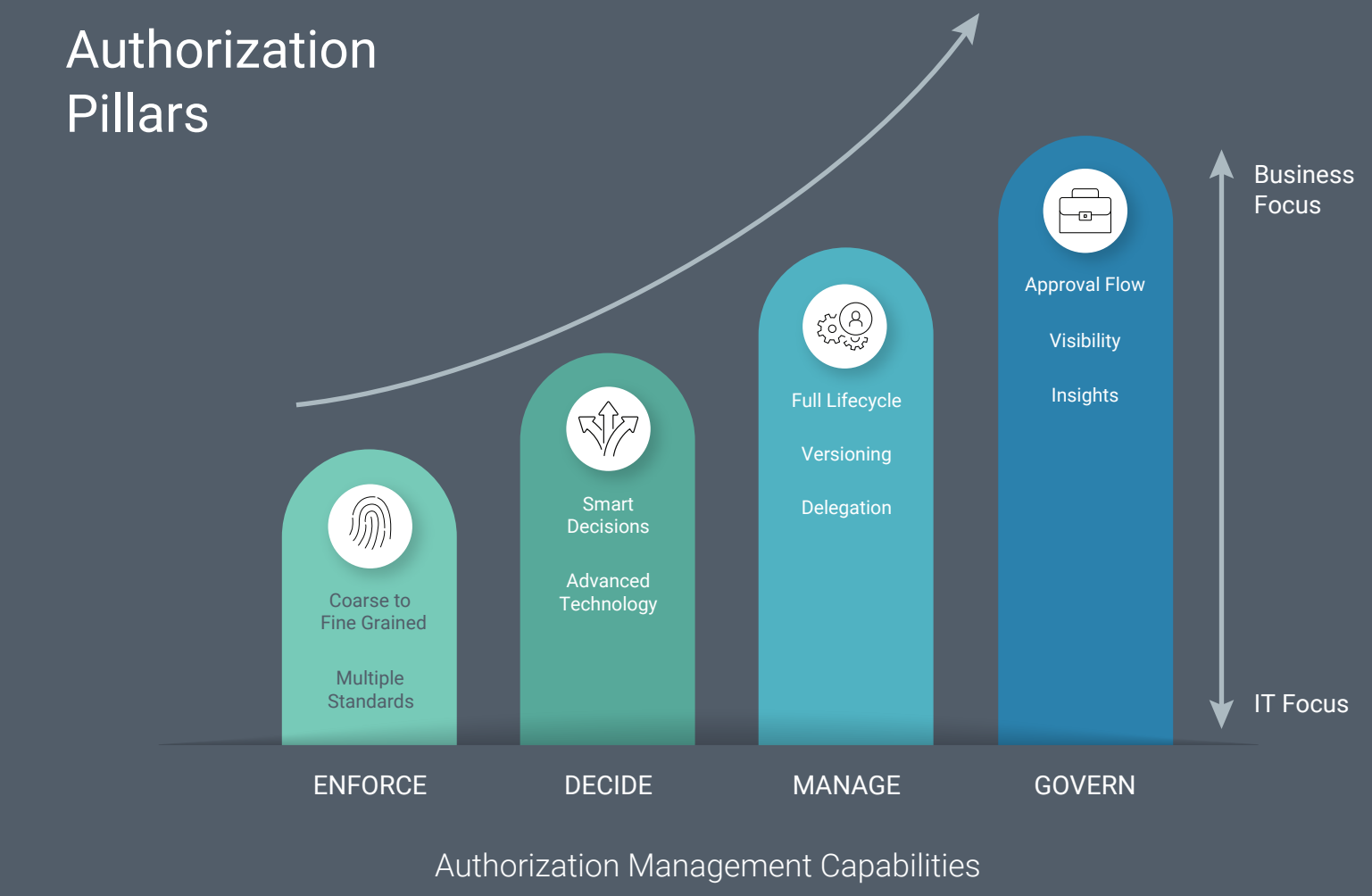
Dynamism

Authorization is responsible for the decisions of who can do what in the app and who can use which resource and data. Because conditions change by the minute, it should be a smart decision. A decision that can consider all relevant information, in real-time. For example: time of day, location where the user is accessing, system changes, organizational changes, or incidents where an organization might be under cyber-attack.

REALISTICALLY…Most applications/systems today use static authorization mechanisms. That means that the decision of who gets to see and use what was made two hours ago, yesterday or the week before, or maybe even years ago...

Numerous Identities

Authorization should be provided to anyone who requires access to data and resources. It can be people, devices, services or things (IoT related). Most solutions today support a single user management, preventing the organization from having a single view of all that can use a specific resource or data.



PlainID Policy Based Access Control Solution

PlainID's comprehensive authorization platform offers the most complete Authorization solution in the market

Business Approach to Authorization

When it comes to Authorization, PlainID recognizes the need to support both worlds, business and technical. A business-oriented language is required to clearly define user access rights and permissions in a way it can be easily described, approved and certified.
The tech side is flexible enough to support what the application or platform requires in order to enforce the right access. **Policy Manager** presents the business owner with a graphical view of the authorization decision, rules and the connection between them to identities, rather than the traditional technical language. In addition, a broad set of APIs offers the flexibility the technology experts require.

Enterprise Ready Solution

Our PBAC Solution is built for the enterprise. It offers a full set of capabilities required to efficiently manage the Authorization lifecycle.

Workflows – Adaptive workflows can be defined for each set of policies or policy building blocks, to approve the policies before deployment.

Version control – Changes in policies are kept and can be reverted to when needed.

Delegated management and SOD control – Management of policies and policy building blocks can be delegated to different stakeholders, enabling an efficient management process and separation of duties where needed.

Controlled deployment – Authorization decisions are deployed in higher environments in a controlled way, after they have gone through an approval cycle.

Real-time Authorizations

Authorizations are determined only when needed. An advanced rule engine is used to "calculate" the authorizations. Time, location, event, risk level and any other attribute can influence the authorizations that a specific entity is granted while accessing the app.

Visual Management

A unique, graphic-based interface is used to represent the connections between entities (people, devices, things, services, etc.). For example: All managers (a rule of "people"), can TRADE in the trading app from office desktops (a rule of "devices"). And they can only MONITOR when working from a tablet.

Analytics and Insights

Our PBAC Solution offers the opportunity to fully explore the effects of each policy in relation to any/all of the Policy's building blocks. Just a small sample of the questions that PlainID's analytical tools can answer would be: Who are the Identities included in the policy? What applications are affected by the policy? What assets can the user access? etc.

Virtual Identities

Our PBAC Solution provides the ability to “see” all identities that require authorizations, within their management platforms. People, Devices, Things and Services, all require and are granted authorizations to enable access to resources and data.

Adoption Tools

Providing just policy-based access decisions is not enough, as organizations are looking for a way to easily adopt those technologies, and optimize their usage.

Policy Manager offers tools to support the adoption process:

Policy Mining – Based on AI and Big Data analytics, the policy mining tool displays the access logic behind the attributes, in addition to addressing the explosion of roles challenge. High correlations can easily be converted to policies in the management studio environment.

Policy Investigate – The Policy Investigate tool enables you to see the full effect of the policy before it is deployed into Production. Using a Sandbox environment, you can see the answers to policy-related questions like: Who are the users this policy relates to? What is received in the consuming app? How will a response change based on different attributes?

Universal Authorization Support

Our PBAC Solution separates the business logic- what we call the Authorization policy - from the technical implementation, thus enabling usage or distribution of the same policy to various consumers. In addition, the PBAC Solution can answer different Authorization requests/ different access patterns with the same policies, keeping a consistency of answers across the various apps. The PBAC Solutions supports all industry leading standards (REST, JWT, XACML, OAuth, etc.) in addition to adaptive integration with leading vendors such as AWS.

SCHEDULE YOUR PERSONALIZED DEMO TODAY TO SEE USE CASES THAT FIT YOUR ENTERPRISE NEEDS.

info@plainid.com www.plainid.com