protiviti®
Global Business Consulting

How can an enterprise use access management to establish a Zero Trust environment?

A hybrid RBAC, ABAC and PBAC framework is the best practice approach

A strong access management program is foundational to establishing a Zero Trust environment by using contextual information to continuously validate that users are who they say they are and by restricting user access to necessary resources only. Within the Zero Trust framework, identity governance and risk-based conditional access controls are identified as the first line of defence against attack.

When establishing effective access governance, organisations must balance audit and security expectations to ensure that users have the appropriate level of access while making sure they can access the resources they need to do their job in a timely manner.

Traditionally, a role-based access control (RBAC) framework has been used exclusively to manage access. RBAC can be complex to design for all access management use cases. It requires a significant level of effort to implement as well as maintenance of a strong governance framework to be effective. RBAC deployments often require manual work from identity access management (IAM) and provisioning teams that often are overburdened. While orchestration technologies and identity governance and administration solutions can provide automation, they alone are insufficient to address the access management challenges currently faced by organisations, including:

- Implementing a Zero Trust approach for all users who need access to resources
- Enforcing granular control to impose data-level restrictions
- Ensuring Day 1 access for new hires
- Managing access to software as a service (SaaS) resources

- Reducing high ticket volumes and time needed for access management and for provisioning teams to assign access
- Eliminating delays in deprovisioning access for movers and leavers
- Overprovisioning access to resources with licenses, resulting in unnecessary costs

To accommodate rapidly changing business needs, an ever-changing technology landscape and the different users who need access (e.g., employees, non-employees, business partners and customers), organisations need a flexible access control framework. Newer technologies have allowed organisations to effectively adopt access control frameworks that complement and build on traditional RBAC, including attribute-based access control (ABAC) and policy-based access control (PBAC). A hybrid RBAC, ABAC and PBAC framework is the best practice approach to establishing risk-based conditional access, effective access governance and a Zero Trust environment. Utilising a hybrid approach of RBAC, ABAC and PBAC allows organisations to address common access management issues.

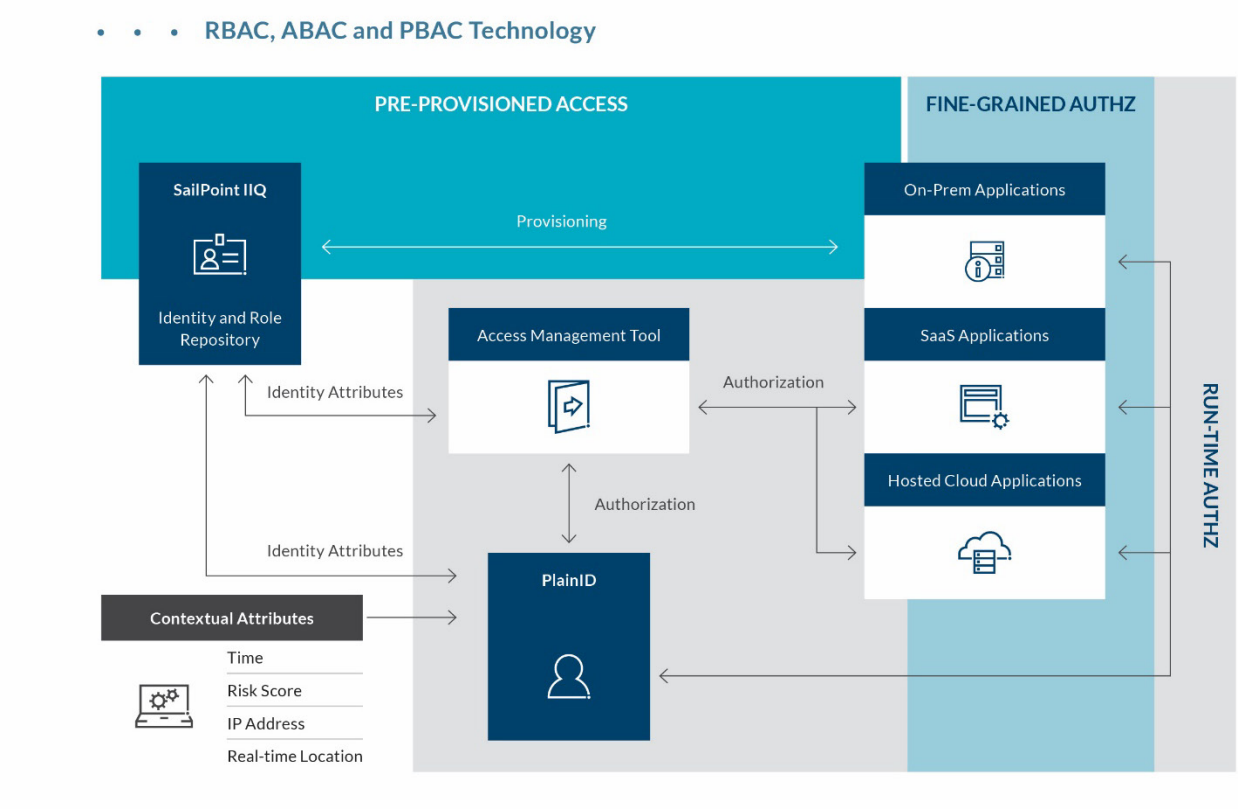
Best Practice – Hybrid RBAC, ABAC and PBAC

The proposed hybrid access control framework leverages the combined strengths of RBAC, ABAC and PBAC access management frameworks. RBAC simplifies access to systems and applications by bundling access into roles. A best practice is to group users with similar job functional access into a single role regardless of job title or other human capital management attributes. RBAC will reduce the number of access requests since managers will be able to request access at the role level instead of specifying specific permissions needed for each system. Access recertifications can be performed at the role level, which will streamline and increase the efficacy of the recertifications. Business-friendly roles will increase transparency of access and will reduce the risk of rubber stamping.

ABAC is a method of regulating user access that dynamically grants users access to systems and applications based on user attributes evaluated at authorisation (when a user attempts to access an application or system). Attributes can also be used to automatically provision or update access ahead of runtime. PBAC further expands on traditional RBAC and ABAC by regulating user access to systems and applications using predefined policies and contextual information that are dynamically evaluated at authorisation.

Both ABAC and PBAC excel in granting birthright access to large swaths of end users (e.g., distribution groups, view access to HR portal, etc.). Attribute and policy-based access does not require manual access provisioning and will lessen the workload of access management teams while ensuring that new hires have access to organisationwide applications on Day 1. PBAC builds off ABAC to provide the same operational gains with much more customisation and granular control of access, including individual data elements. Runtime authorisation removes the need to provision access to users. Instead, the appropriate level of authorisation is calculated

and passed to the target system when the user accesses the application. Contextual information such as IP address, location and risk score can be ingested in real time and used as inputs to the authorisation decision, ensuring Zero Trust principles are enforced.



The above diagram outlines one best-practice architecture that leverages the combined strengths of RBAC, ABAC and PBAC to address common access management use cases. Implementing the recommended hybrid access management framework is best accomplished by using three key identity and access management technologies to address several common use cases:

1. **SailPoint** – A leader in the identity governance and administration space that acts as a comprehensive identity repository, governance engine, role catalogue and provisioning engine.
2. **Access management technologies (e.g., Okta, Ping, etc.)** – Authentication providers that can be used to provision real-time access to web-based applications.
3. **PlainID** – A leader in PBAC used to make real-time granular access decisions and grant authorisations in real time to both on-premises and web-based applications.

In this model, SailPoint is the source of truth for both identities and identity attributes which can be dynamically used by access management tools and PlainID as an input for authentication and authorisation decisions in real time. Organisations should leverage SailPoint's governance

capabilities to manage access and use its role catalogue and strong provisioning capabilities to pre-provision job functional role-based access to applications where possible. SailPoint's identity lifecycle capabilities should be leveraged to ensure the deprovisioning of roles and downstream access on mover and leaver events.

Access management tools should continue to be used where possible to manage authentication and support authorisation for application-level access. The authentication or authorisation groups can be provisioned by SailPoint. Many access management tools now have just-in-time provisioning capabilities. The transition to a Zero Trust framework is predicated on implementing technology that enables runtime authentication and authorisation decisions. Where possible, the just-in-time provisioning capabilities of access management tools should be used to dynamically provision authentication groups where user attributes drive who should have access.

As a robust PBAC solution, PlainID should be used to authorise access within both on-premises and cloud applications where clear rules and policies can be defined to determine access levels. The real-time policy evaluation is the key functionality that enables Zero Trust and prevents unauthorised users from accessing integrated systems. Recommended use cases include using PlainID to grant birthright access to applications across the enterprise and ensuring end users have access to the resources on Day 1. Since these policies are applied at runtime, PlainID can eliminate the need to request access for integrated systems and drastically reduce the time needed to provision access.

The other notable benefit of PlainID is fine-grained access control, enabling identity teams to include data-level security and control specific actions (e.g., assigning an expense approval threshold based on the user's current level in the organisation) within a centralised policy engine. In a traditional RBAC model, breaking down entitlements to include data-level security is not feasible and can bring about a bloated and unmanageable entitlement catalogue. PlainID navigates around this issue by checking attributes for both the end user and asset (i.e., the resource within the target application that users are accessing) to allow for streamlined access decisions based off a pre-set set of "conditions" that contextualise the access authorisation at runtime.

Where possible, PlainID can be used to manage access to applications with licensing restrictions. The runtime authorisation functionality, along with just-in-time provisioning capabilities of the access management tool, will help ensure those who need access to licensed applications have access to them without the risk of over-provisioning licenses to users who don't use that access regularly but are allowed access when needed.

Illustration of how the hybrid RBAC, ABAC and PBAC model can be deployed:

- When a new accounts receivable (AR) manager in the Southeast region is hired, the accounts receivable director will submit a request for the AR job role to be assigned to the new manager.
- SailPoint IQ will assign the job role and pre-provision the access mapped to the job role, which may include the ability to create AR invoices in the ERP solution and access to revenue reports in the reporting tool.
- On Day 1, the AR manager will also be able to access resources integrated with PlainID if the manager meets all criteria defined in policies that govern access to the resources.
- If the organisation has defined a granular access policy where all employees at a manager level or above can access Salesforce but can only view information in their region during business hours from 9 p.m. to 5 p.m., PlainID will evaluate the policy in real time and will determine if the user is permitted to access the application and what the user is able to do in the application.
- In this scenario, when the AR manager attempts to access Salesforce during business hours, PlainID will automatically approve the real-time request from the application or access management tool to allow the manager access to view records for Southeast region clients.

Leveraging the combined strengths of a hybrid access control framework addresses many access management challenges currently faced by organisations by granting greater control around end-user access while lessening the burden on IAM teams and ensuring that end users have the appropriate level of access in a timely manner. A key step in the Zero Trust journey is the implementation of a hybrid RBAC/ABAC/PBAC approach, leveraging runtime authorisation decisions whenever possible.

How Protiviti Can Help

Protiviti's RBAC team has extensive experience assisting clients with their strategy and governance frameworks, as well as with designing and deploying role-based access controls for enterprises in all industries. Designing roles is more of an art than a science. Protiviti's services help organisations sidestep pitfalls faced by companies with traditional RBAC models, especially in the area of role governance, and can help implement access management frameworks and technologies that adhere to Zero Trust principles.

Protiviti's services include:

- Strategy and roadmap – RBAC/ABAC/PBAC
- Governance framework – RBAC/ABAC/PBAC
- Role design/engineering
- Policy authoring/design
- Entitlement management
- Managed RBAC/PBAC services

Contacts

Willy Alvarado
Director
+1.407.460.8673
willy.alvarado@protiviti.com

Brian Isserman
Senior Manager
+1.850.712.9290
brian.isserman@protiviti.com