Solution Brief

THALES

CYBERSECURITY

Thales Policy-Based Authorization Manager

OneWelcome Identity Platform

PBAC-Powered Dynamic Authorization for the Enterprise

cpl.thalesgroup.com

THALES

CYBERSECURITY

Authentication establishes identity. Authorization governs what that identity is permitted to do — to which digital resources, through which actions, and under what conditions. Policy-Based Access Control (PBAC) makes this a business decision, not a development problem. Policies define who can access what, and under which conditions, using business-readable language evaluated dynamically at runtime against connected identity and attribute sources, and enforced consistently across every layer of the technology stack — APIs, microservices, data platforms, and applications — without embedding authorization logic in application code.

Thales Policy-Based Authorization Manager (PBAM), part of the OneWelcome Identity Platform, delivers PBAC-governed Dynamic Authorization for organizations that require consistent, fine-grained, and auditable access control across complex regulated environments.

The Business Challenge

As organizations shift to API-first and cloud-native delivery models, authorization complexity compounds with scale. The root causes are structural:

- Static RBAC models cannot express fine-grained subject, resource, and condition-based precision — roles proliferate, entitlements sprawl, and demonstrating least privilege becomes impossible
- Authorization logic embedded in application code couples policy change to software releases, not business decisions — slowing response to regulatory and operational change
- Coarse-grained enforcement at the API layer does not extend to the underlying resource — the account record, transaction, or data field — leaving critical protection gaps
- No consolidated visibility across policies means compliance teams cannot trace access paths, satisfy audit requirements, or demonstrate control effectiveness
- Without Zero Standing Privileges enforcement, persistent role-based access creates unnecessary blast radius when identities are compromised
- Regulatory mandates — PSD2 SCA, DORA, FFIEC layered controls, GDPR data minimization — require demonstrable, policy-driven access governance that role assignments alone cannot deliver

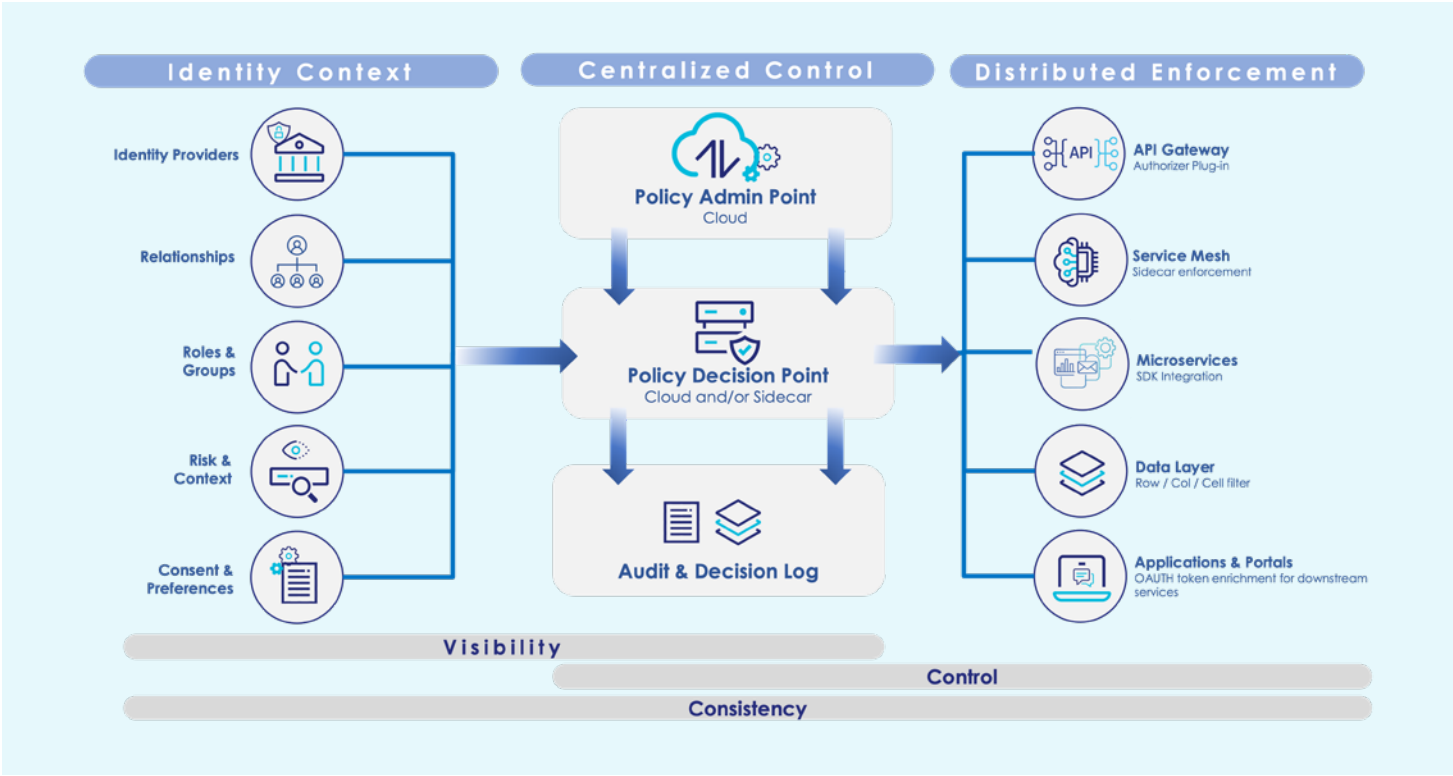
The Thales PBAM Solution

PBAM delivers Dynamic Authorization through a PBAC framework in which Access Policies define who can access what, and under which conditions — evaluated in real time by the policy evaluation engine against connected identity and attribute sources. Runtime-evaluated identity groups — sets of identities matched to policy criteria at the moment of each access request — replace static role assignments, enabling Zero Standing Privileges enforcement without pre-provisioned group membership.

PBAM can also federate to existing customer identity providers via OIDC, leveraging those sources without replicating user directories or creating additional identity silos. PBAM is a pure authorization layer, complementing IAM and CIAM investments rather than displacing them.

Key Business Benefits

Business Benefit	What It Enables
Policy Agility	Respond to regulatory and business change at policy speed — update Access Policies without redeploying applications or modifying application code
Consistent Enforcement	Eliminate authorization gaps by enforcing PBAC-driven decisions uniformly across APIs, microservices, data services, and applications via distributed pre-built enforcement integrations
Audit Readiness	Business-readable authorization decision records provide traceable, evidence-based assurance that satisfies auditors, compliance teams, and regulators
Reduced Development Overhead	Externalize authorization from application code through composable, reusable Access Policies — reducing implementation effort and eliminating per-application authorization logic
Zero Standing Privileges	Replace persistent role assignments with runtime-evaluated identity groups — granting access dynamically based on current identity context, not standing entitlements
Digital Agility	Accelerate adoption across APIs, cloud-native services, and data platforms with out-of-the-box pre-built enforcement integrations that enforce policy without infrastructure replacement



Centralized Management, Distributed Enforcement

PBAM enforces Access Policies at every, or several layers by the policy admin's choice, of the technology stack through a growing ecosystem of pre-built enforcement integrations — deployed at API gateways, service mesh, and application integration points. Enforcement integrations intercept authorization requests, query the policy evaluation engine, and enforce the resulting Allow or Deny decision without any authorization logic residing in the application itself.

For data use cases, enforcement extends to the data service layer. The policy evaluation engine returns a resolution translated into a data filtering clause, enabling row-, column-, and cell-level access control enforced dynamically at query time — ensuring identities receive only the data their policy context entitles them to.

Token-based enrichment is also supported for downstream services consuming enriched OAuth tokens, delivering PBAC-governed access decisions with minimal integration effort.

These enforcement patterns are composable. Organizations apply different enforcement configurations across different parts of their technology stack and evolve their authorization architecture incrementally — without replacing existing infrastructure.

Dynamic Authorization

- PBAC-powered policy evaluation engine with real-time authorization decisions
- Subject, resource, and condition-based Access Policies with runtime-evaluated identity groups
- Fine-grained authorization at the resource and data level
- Row, column, and cell-level data filtering
- Zero Standing Privileges enforcement
- Pre-built enforcement integrations for APIs, microservices, and data platforms

Policy Management & Governance

- Centralized policy authoring in business-readable language
- Consolidated policy visibility across all policies, resources, and identities
- Policy-as-Code with CI/CD pipeline integration
- Approval workflows and policy lifecycle management
- Business-readable authorization decision records for audit
- Separation of duties across authoring, admin, and audit roles

Target Use Cases

- API authorization — access decisions enforced at the resource level (account, transaction, customer record), not just the API endpoint
- Data access control — row, column, and cell-level filtering governed by Access Policies, not application logic, across databases and data lakes
- RBAC modernization — replacing role explosion with composable PBAC policies that express actual business logic and can be authored without developer involvement

Why Thales

Thales PBAM brings PBAC-governed Dynamic Authorization to the OneWelcome Identity Platform — built for the authorization challenges that enterprise-scale, regulated digital services actually face. Centralized Management with Distributed Enforcement is a first-class architectural principle: Access Policies are authored and governed in one place; pre-built enforcement integrations enforce them across every API, microservice, application, and data service in the environment. Consolidated policy visibility, business-readable decision records, and an incremental adoption model give security, compliance, and business teams the governance foundation that authentication alone cannot provide.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us