WHITEPAPER

Build vs Buy:

A Guide to Evaluating Authorization

Supported by The Cyber Hut

plainID

Table of Contents

What is Modern Authorization Management?

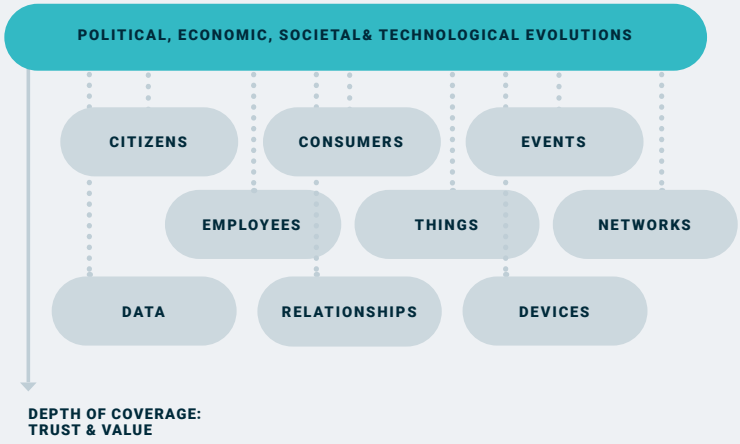
THE BACKSTORY - BUSINESS CHALLENGES

The modern organization is facing numerous challenges as it looks to enable a highly distributed and often complex workforce of full time, contractor and third party workers, whilst simultaneously engaging an ever growing external user community of online customers and consumers of information.

THE IDENTITY OF EVERYTHING, EVERYWHERE

The digital-first enterprise needs to empower these different user communities, whilst responding to competitive pressures - often having to operate with only limited asymmetric information - which requires an ability to fail fast when it comes to launching new products, services and applications.

The continued evolution of digitization is driving us towards an “identity of everything, everywhere” model - requiring organizations to manage the “who has access to what” on an enormous scale - cutting across different user communities, data structures, relationships and events.



EVOLVING TECHNOLOGY LANDSCAPE

Technology changes - new problems emerge which existing infrastructure and tooling can no longer solve - and existing solutions incrementally and radically innovate - which allows existing problems to be solved faster, cheaper and with less effort.

Today's enterprise needs to leverage, integrate and consume services from a range of cloud providers, build services and applications using APIs, microservices and existing infrastructure while upholding privacy and security controls for various different data types. Siloed identity, application delivery and protection mechanisms can no longer deliver the capabilities needed to allow for business growth, agility and competitiveness.

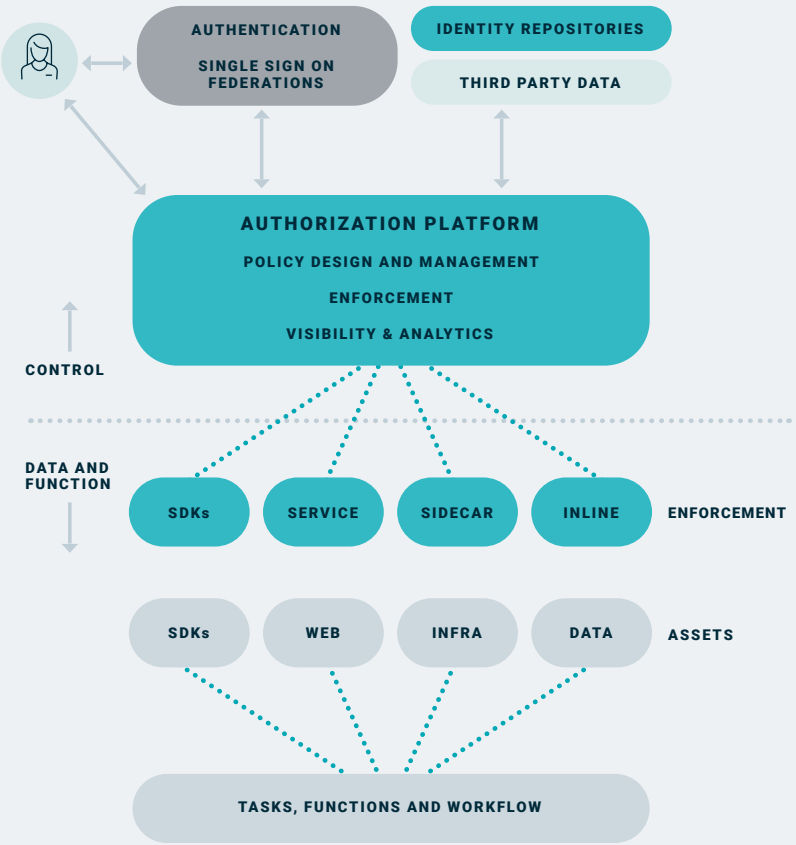
EXTERNALIZING AUTHORIZATION

Authorization - the ability to define and enforce who has access to what - has typically been the forgotten gambit of the AAA triad (with Authentication and Accounting being the remaining two) - with access control logic taking second place behind how user's login. Any access control service that did exist, was often tightly coupled inside an application or perhaps supplied via a coarse grained model as part of the single sign on and session management platform.

Today, authorization has become a first class citizen when it comes to the identity and access management (IAM) services available to business leaders. Specialist authorization platforms are now available to provide an external set of capabilities covering policy design, enforcement, analytics and reporting.

This unbundling of the IAM market into devolved specialist services allows application and service builders to focus on what they do best- understand the business and deliver value - instead of developing bespoke identity and security solutions.

The authorization platform needs the ability to deliver access control services to a range of different user communities - consumers, workforce and third parties at a minimum - as well as being able to protect a range of different asset types - from APIs and microservices - through to raw data objects and payloads. Visibility - of both policies and who has access to what - also needs to cater to a broad array of interested stakeholders - from security architects and developers through to business leaders and application owners.



CENTRALIZED MANAGEMENT & CONTROL

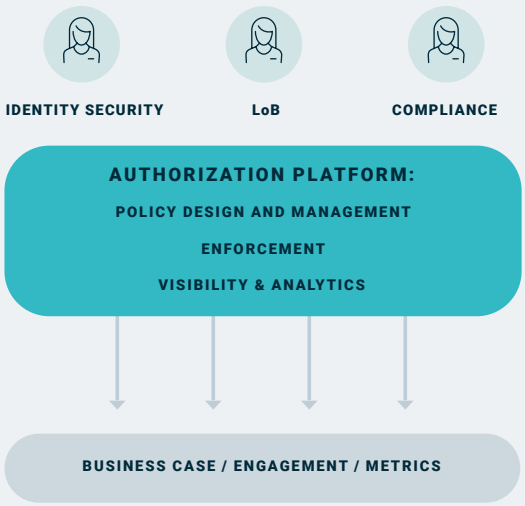
An immediate benefit of a centralized management and control platform is to help engage and inform those different stakeholders within the business - by expanding the authorization service potential via internal evangelism and business case creation but also via acceleration of application onboarding and policy creation and management.

As authorization has become a broader IAM strategic tool it needs to be used to protect a range of assets - in different lines of business (LoB) - each with different metrics and success criteria. In some ways authorization is moving from being an isolated and specialist feature, to a more broad reaching and generic service, which requires the ability to engage and provide value to different personas with different security requirements.

An evolutionary aspect of this is the ability to leverage a policy based approach to asset protection - with an ability to integrate the principles of role based access control (RBAC) and the more agile attribute based access control (ABAC) simultaneously. Policies allow for reusable components that can accelerate application security roll out and also provide consistent and compliant ways to enforce security controls.

However, today's broad array of assets that need protection, requires a wide range of policy models - including business related data, persistent profile data, groups, attributes and runtime context.

Policy based access control (PBAC) provides the foundation for governance, version control and management, yet it could also provide the ability to overlay and extend existing access control methodologies.



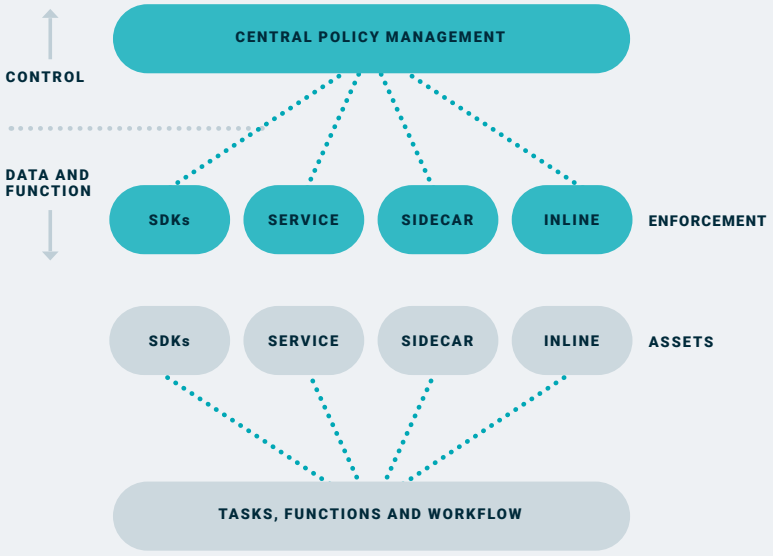
DISTRIBUTED ENFORCEMENT

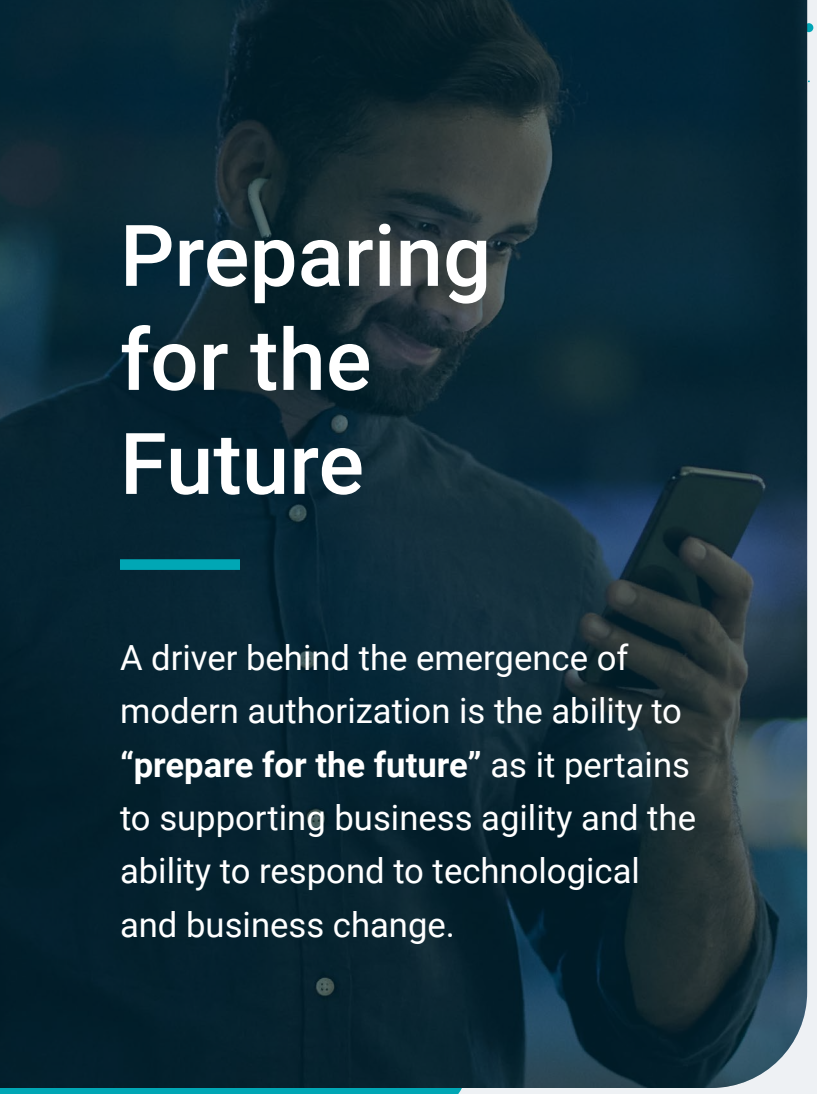
The modern enterprise is powered by data - data supplied to numerous application types and services - from APIs and microservices, to web portals, databases and third party applications. These information “assets” are continually evolving and are located in a dispersed set of physical locations - with different operational owners and security requirements. The centrally managed controls need to be upheld against this varying set of services - via a range of enforcement and decision services - from native APIs, SDKs, inline services.

The “data plane” enforcement points will need to have access to the centrally authored policies - either via direct callout or perhaps via a more asynchronous pull down of the necessary rule data.

A main requirement of this layer is the ability to provide protection to an ever growing variety of systems and applications - whilst providing consistent enforcement of both persistent and runtime

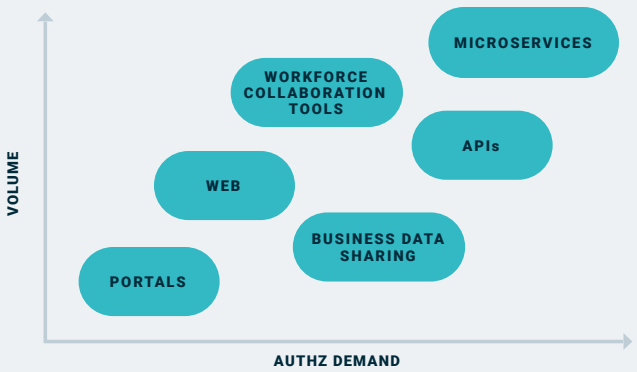
Enforcement is also likely to involve fine grained authorization (FGA) controls - that start to extend and expand the traditional approach of leveraging just persistent identity and directory data such as roles and groups. Whilst persistent data plays a role in establishing access control baselines, today’s security requirements are more reliant on adaptive controls - leveraging runtime context - to provide per request, per field or per attribute style dynamic access based on these more volatile pieces of information.





Preparing for the Future

A driver behind the emergence of modern authorization is the ability to **“prepare for the future”** as it pertains to supporting business agility and the ability to respond to technological and business change.



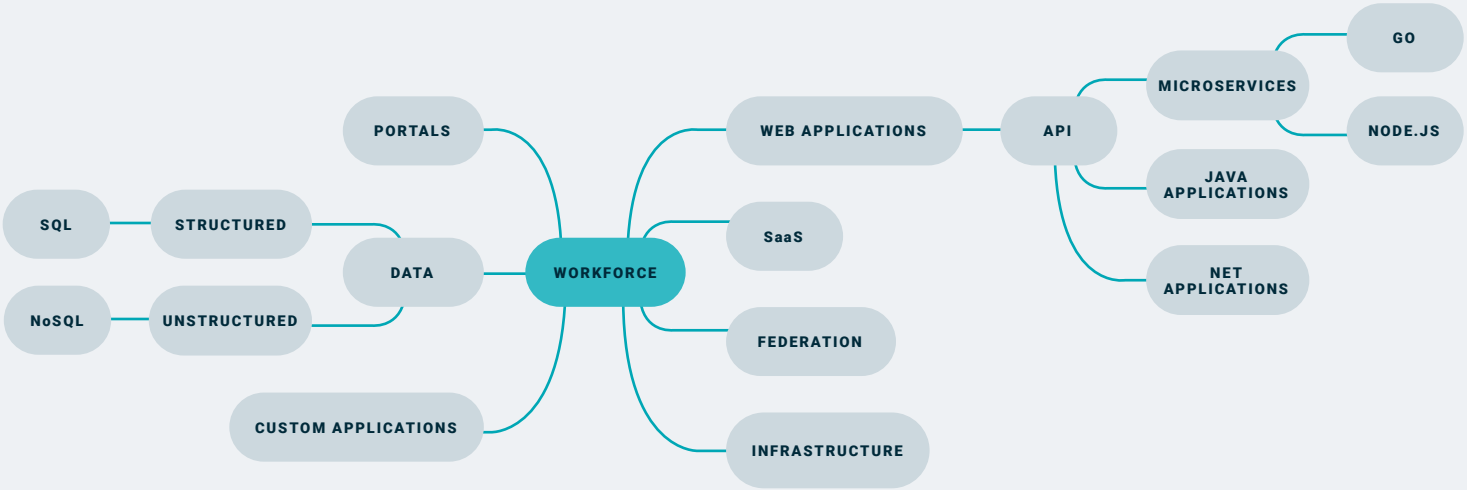
APPLICATION VOLUME

The modern enterprise needs to cater to an ever increasing need to support a variety of business applications - some homegrown and custom, others more generic such as cloud services and reusable API components.

From the protection of existing web applications and portals, through to newer requirements focused on the protection of high volume APIs and infrastructure components such as service meshes, authorization services need to be deployed to more corners of the workforce enablement landscape.

Not only is the volume of particular asset types increasing, those assets are also demanding authorization capabilities for the first time. APIs, microservices, infrastructure components and data objects no longer wish to be tied by custom and siloed access control solutions.

The number and type of applications, workforce data sharing opportunities and PII collection and management capabilities is increasing. A decoupled and repeatable approach to providing authorization services based on reusable components is essential to support the ever changing business landscape.



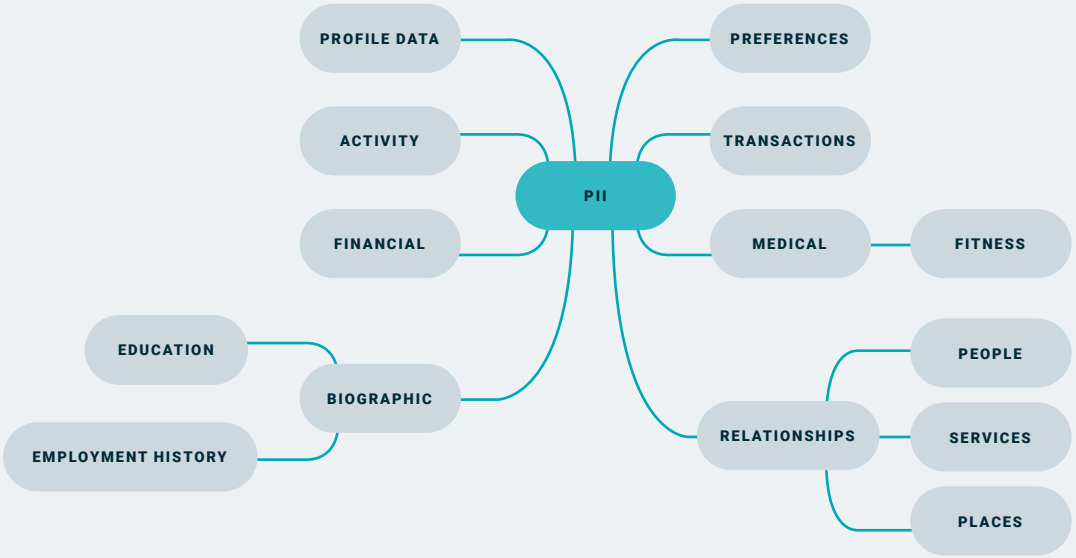
DATA VOLUME

Whilst data protection was often the purview of data management teams, data as “the new oil” is permeating to all parts of both the internal workforce and external facing parts of business interactions.

The rise of PII (personal identifiable information) collection, storage and processing for the enablement of consumer services has raised the bar with respect to data compliance adherence as well as the need to provide data sharing and revocation capabilities that could allow privacy to be seen as a competitive advantage.

In addition to the more traditional forms of PII such as biographic and financial service records, we are now seeing preferences, activity and medical data being collected and aggregated by the extended arm of consumer IoT devices, bloating the cloud side storage and processing facilities. That data needs protecting, with flexible approaches to privacy enablement - and more importantly timely access revocation.

All of those services rely on authorization and specialist platforms to deliver those capabilities resulting in faster application deployment time, using reusable components and governance patterns.



DEPLOYMENT PATTERNS

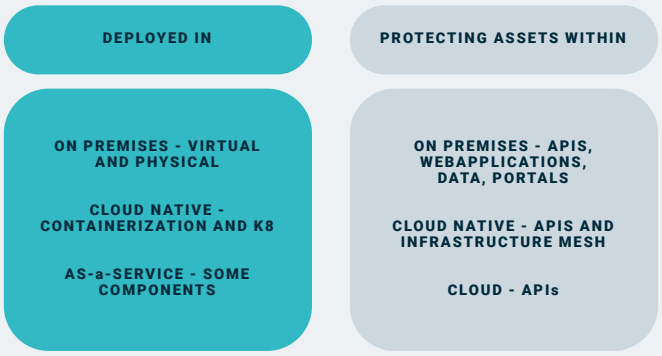
Finally modern authorization capabilities need to be both deployed in and be able to protect assets within a broad array of deployment environments - including hybrid cloud environments, cloud native environments and existing on-premises infrastructure.

HYBRID CLOUD

The “hybrid cloud” journey will see organizations leveraging a range of cloud service providers (CSPs) to deliver core infrastructure components as well as leveraging cloud as-a-service components for more specialist services. Core authorization capabilities will need to operate against an ever increasing variety of cloud models.

CLOUD NATIVE

“Cloud native” can be readily defined as components which may well be being deployed in controlled environments such as private clouds or even on-premises, but leverage the characteristics of a cloud ecosystem - such as being orchestrated, scalable, highly available and available on demand. Many of these “cloud native” ecosystems build heavily on containerization with the likes of Kubernetes for container management.



IN SUMMARY

The modern enterprise is both deploying its core services into a broad array of deployment ecosystems - each with differing constraints and operational boundaries - as well as consuming services from a similar broad ecosystem. Authorization and access control services - and the supporting policy management, permissions and analytics - need to be readily available to be both deployed and consumed in these ecosystems too. Flexibility in deployment architecture is key to helping to support business agility and technology modularity.

The Limitations of Homegrown Solutions

- Inability to Extend
- Hardcoded Users & Permissions
- Stale & Excessive Permissions
- Lack of Cross-System Visibility
- Lack of Repeatability
- Lack of Governance

As the modern enterprise architecture demands a more decoupled and agile approach to authorization and the core services that it brings, the existing access control deployments - often tightly coupled and embedded within enterprise applications - can no longer provide the level of agility, correct feature set and coverage the business assets need.

INABILITY TO EXTEND

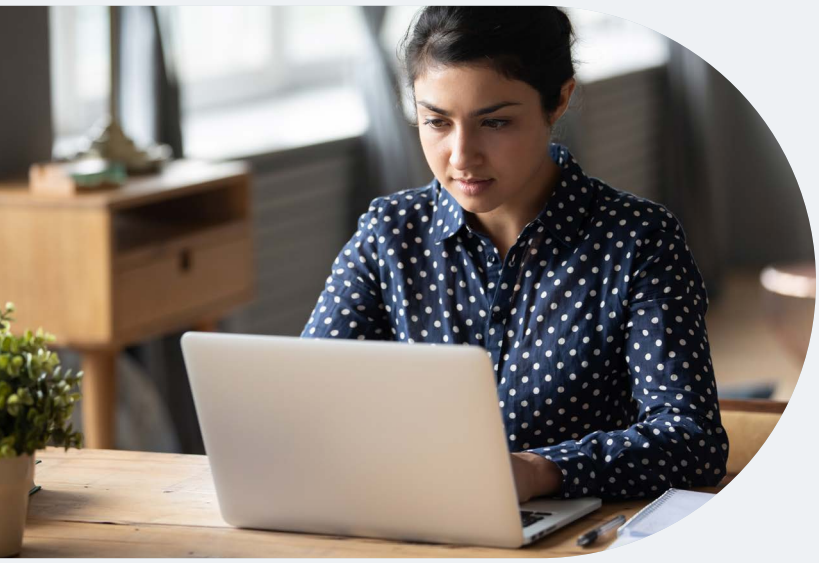
A key requirement of any modern decoupled identity and access management service component is the need to extend and expand - both horizontally and vertically. From a horizontal perspective, the need to add functionality, features and customization is key in order to improve the flexibility of the service being offered. From a vertical perspective, we need to consider how the authorization services can be delivered to a wide coverage area with varying levels of integration. Often custom authorization solutions provide protection at the web tier, based on hard coded usernames or groups. Any alteration to the runtime protection requirements or to the level of where enforcement is taking place, requires huge operational effort - often requiring application redesign.

LACK OF REUSABLE COMPONENTS

In the DevOps oriented infrastructure deployment world, reusable components allow for the rapid roll out of new services and applications, but also provide a baseline for governance, security control and operational management. Homegrown authorization solutions - whilst perhaps delivering excellent functionality - may well be classified as bespoke, with each implementation being customized. Customized during design, customized during implementation and customized during daily operations. The ability to replicate the design and process to other systems becomes limited, resulting in more operational overhead and more siloed systems.

LACK OF VISIBILITY

A major consequence of siloed and customized deployments is a lack of centralized visibility pertaining to who has access to what and how those permissions are being managed. Individual projects built using homegrown tools and practices are often owned and managed at an application or department level. Daily management is focused on single applications and processes, resulting in a coverage gap regarding analytics and an inability to identify patterns and usage metrics.



OPEN POLICY AGENT - A GREAT START BUT NEEDS SUPPORT - A common component being utilized for many homegrown solutions is Open Policy Agent (OPA) - a popular open source project that provides fine grained policy support via a declarative policy language and lightweight broadly deployable decision engine.

OPA provides huge advantages to hand-cranking authorization components, but effort is still needed in the larger scale production focused projects. Whilst OPA is comfortable with being deployed for the protection of infrastructure assets, rule data still needs to be created, managed and distributed. The power of modern externalized access control will come from the ability to create access control policy that can cover a range of resources, subjects and actions and be extensible in order to cover future authorization requirements, above and beyond the typical infrastructure protection landscape.

An ability to centralize the OPA policy design and management components is important, as is the ability to distribute the created policy definitions to a widely deployed set of OPA instances. This distributed process should be repeatable using reusable components and comply with modern devops processes such as being programmatic and automated.

The Cost of Doing Nothing

Existing home grown authorization solutions - based on open source components or in house libraries - are often “doing just enough”. As is typically the case with many identity and access management components that are built in house, the short term status-quo can often overshadow the longer term strategic benefit of moving to more specialist platforms.

THE OPPORTUNITY COST

A decision to “do nothing” is still a decision. The opportunity cost - the loss of missing out on other options - is significant as it pertains to authorization and access control. Modern authorization can help support business agility - by allowing new services to be rolled out quicker and data to be shared to third parties more securely. The end result is a more competitive and responsive set of business services that delivers the correct access to the correct people at the correct time. Authorization can essentially be seen as a business enabler and sticking with home grown solutions that are often static in their position of development hinders that enablement.

THE OPERATIONAL COST

The support and personnel costs of having to manage bespoke homegrown solutions are significant. The creation of any software asset that can’t be sold on directly to an end customer, can immediately become a liability - requiring specialist personnel to support its development and day to day operations. Extending and upgrading existing access control solutions (even if possible) will require highly skilled architects and developers to alter code, write policies and understand application-specific access control logic. Those personnel costs could be diverted to tasks more aligned with generating business value within the application supply chain.

ENTERPRISE RISK

The security risks to the modern enterprise are large and rising. The number of data breaches is growing yearly and the breadth of attack vectors and complexity of attacks increases the need for improved security visibility with the ability to iterate and improve security controls annually. This may not be possible with homegrown solutions that were often focused on tactical business problems. A lack of roadmapping and modular design can increase business risk by not being in a position to respond to emerging threats and attack patterns

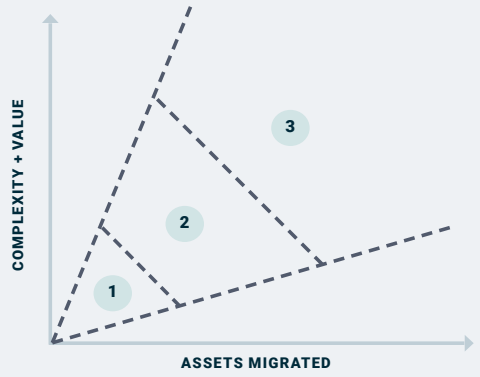
Business Case & Evaluation of CoTS

The migration to a commercial off the shelf (CoTS) solution is a strategic investment and will benefit the business via a cascading effect of improved agility, a more robust and repeatable security posture and reduced operational cost and complexity. However as with any strategic change, the internal business case, the evolution of commercial offerings takes time and effort.

The first aspect of building a cross-functional and multi-asset business case for authorization, is to understand the entire access control landscape, whilst focusing on delivering smaller and iterative pieces of business value. Attempting to deliver an entire authorization platform from day one, is likely to result in a slower planning cycle, be less responsive to new use cases and be unable to capture and process stakeholder feedback. By focusing on a smaller set of applications and use cases on day 1, allows the technical and business process knowledge to be collected and analyzed in a way that is responsive and agile. During stage 1, by selectively focusing on applications with simpler access control logic, smaller groups of users or perhaps limited contextual processing, allows the platform design to be consumed in a much more efficient manner with less impact on daily operations - whilst simultaneously creating improvements in efficiency and operations that help boost confidence in the longer term strategic aims. By the time the most complex applications are to be included in the overall roll out plan, functional and non-functional capabilities are well understood, and onboarding and customization processes streamlined and automated.

BUILDING A BUSINESS CASE

- **Small Start to a Large Finish**
- **Selective Application Onboarding**
- **Capability Assessment**



Evaluation of CoTS

Once the existing application protection landscape is well understood and a potential capability and migration process drafted, a process to analyze CoTS technologies becomes considerably easier. Engagement with a commercial supplier should involve understanding not only internal requirements and coverage needs, but also the capabilities of the vendor and what is needed to deliver a modern authorization solution.

CAPABILITY	GUIDANCE
Platform Approach	• Does the vendor provide a specialized centralized platform wide approach to authorization management - that allows for the support of immediate use cases, but also looks to the future, with respect to extensibility, extension points and customization?
Policy Management	• The capturing of access control logic into policies is common - can the vendor provide a basic set of policy management tools, that allow the lifecycle management of policies - including strong change management and governance features? • Are policies accessible by a range of different stakeholders - from application and security architects, through to line of business owners and non-technical functional leaders?
Policy Design	• How are policies designed within the authorization platform? • Does the platform integrate a range of data sources during the policy design process - from static identity and permissions data (groups, roles, identity profile attributes) through to more volatile data covering the context of the transaction, history and environment? • Can policies be created programatically as well as by non-technical members of the business?
Enforcement	• How is policy data enforced with respect to enabling a broad array of asset protection options? • Does the enforcement involve event decision making (by having access to a central policy decision point, or being able to make decisions locally) and by being available to a range of different asset types and flow scenarios - including inline, as a service and via SOK/ API integration?
Deployment Acceleration	• Does the platform aim for broad global coverage and provide methods to accelerate deployability - with limited deployment dependencies (ability to work on-premise, in private or public clouds)? • Can the platform be deployed in an automated and programmatic fashion, that can leverage reusable components and processes?

Calls to Action

Authorization has become a critical component of the modern enterprise - delivering business agility via the flexible security of critical data and information assets. Homegrown access control solutions are common - either embedded within complex systems due to bespoke requirements or due to a legacy view of CoTS providers - but are failing to deliver against modern requirements that support agility, repeatability and broad coverage.

- **Identify The Problems**
  It is important to identify and have visibility into the range of assets, applications and access control logic that will form part of the next generation authorization solution for your organization. Landscape mapping, capability analysis and visibility into existing authorization and access control solutions helps to understand the immediate and future requirements associated with critical information systems protection.

- **Prioritize**
  Not all existing and future assets will need the same level of security at the same time. It is critical that the correct systems not only have the correct level of protection, but they must also be integrated into the correct architecture at the right time. Prioritization should include not only immediate needs and how those needs are fulfilled but also a look to future requirements that will impact the business over a 6-24 month period. Competitive pressure, emerging security threats and business agility should all be considered when looking at the migration pattern and future authorization demands of existing systems.

- **Research & Assess**
  Authorization can be a complex array of tools, implementation architectures and integration options. Research and assessment of both homegrown and commercially available solutions is critical to developing a future capability that supports the ever changing business needs associated with employee and customer data assets.

HOMEGROWN - BENEFITS	HOMEGROWN - COSTS	CoTS - BENEFITS	CoTS- COSTS
Ability to deliver bespoke solutions	Lack of best practice and skills	Specialized product	Higher initial cost
Ability to start fast	Long term supportability and expertise staffing	Features and capabilities evolve and track the industry	Change in practices
Specialist Knowledge - IP asset	Ability to respond to future changes and growth	Secure and scalable tooling	Migration effort
Lower Initial fixed cost	Cost of personnel	Risk is outsourced	Training and support effort

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.**