



WHITE PAPER

Key Considerations: Using Dynamic Authorization to Optimize Policy Building

Background

An organization's cybersecurity infrastructure is built on a robust set of policies that ensure the right information is accessed by the right people at the right time. At the center of these policies are authorization permissions that control all layers of the application (front-end windows, APIs and underlying databases). The discussion of how to build a strong authorization policy is foundational to a modern cyber security strategy.

Traditionally, organizations took a centralized approach to policy building based on singular attributes such as applications and roles. But this approach has limitations and is challenging to maintain as businesses become increasingly more dynamic.

With the growth of an organization came the expansion of applications being built or licensed and the evolving nuances of various roles. Organizations also began adapting to cloud-based environments with more apps and more data, which necessitated the transformation of policies.

Businesses need a new way to build their cybersecurity foundation. Dynamic authorization is a dynamic policy model that centralizes accountability while decentralizing policy authoring. While the Chief Information Security Officers (CISOs) and/or identity leaders remain at the center of the strategy, their role is to remain accountable for the successful deployment of the authorization process and ensure the policy incorporates the full scope of business needs across the organization (Fig. 1). Policies need to reflect a broader identity and security strategy, and this starts with understanding the dynamic authorization process.

The following captures key considerations your organization should review to reflect the broader identity and security strategy of an dynamic authorization process.

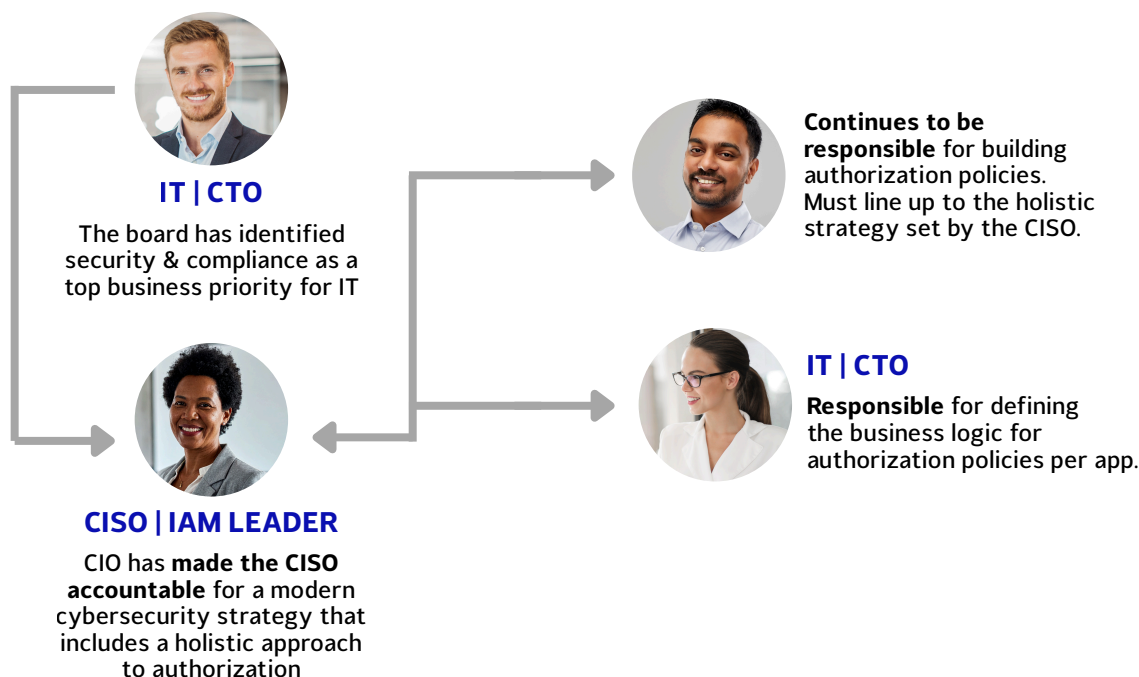


FIG.1

Building Policy-driven authorization

Strong policies are built using a dynamic approach to authorization model (Fig. 2). This model is the foundation for building a Zero Trust policy, which continuously validates permissions for each user based on a set of attributes (who, what, where, when, why and how). Taking a Zero Trust approach to policy building eliminates absolute trust from the equation by continuously validating users at all layers of the application. A policy-based authorization approach requires several key elements, which are obtained through the policy modelling process.

There are five key phases of a policy modelling process to achieve a framework that eliminates trust from the equation by continuously validating users at all layers of the application.

The policy modelling process identifies contextual attributes that enable access to data through a range of applications. These attributes can be modified, and put into action in an efficient and timely manner.

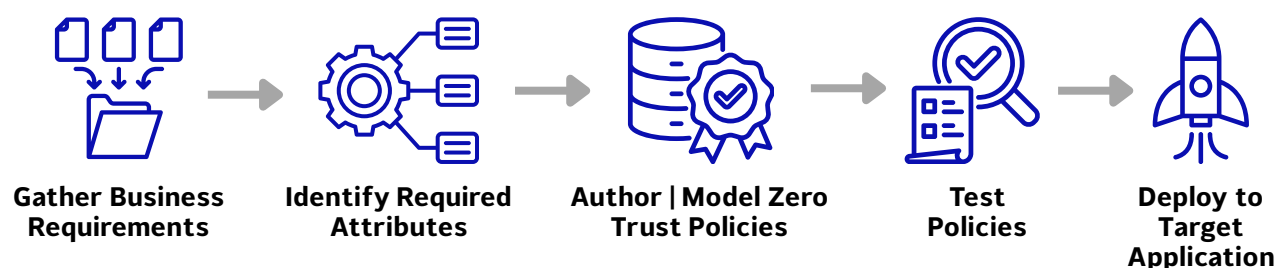


FIG.2

Dynamic attributes in policy modelling

Policy attributes can differ based on various factors within an organization. For example, a small organization may list the data access specific to certain roles, while a larger organization may have more complex breakdowns between organizational, application-specific or departmental policies. A dynamic approach to policy building requires the attribute values to be the sole modifiable element. They determine policy decisions and outcomes in an attribute-based access control (ABAC) environment, which focuses on safeguarding data in applications, databases, microservices and APIs, within complex architecture.

An example of an attribute value is user type, which was once the sole attribute in a policy. Now, it is one of many that are combined to determine the correct access path for an employee.

In other words, all attributes must align to validate the user as they attempt to access certain data. The type of access they have can change based on whether they apply to certain attribute values, but not the policy itself. Centralizing permission information based on attributes also abolishes the manual collection of audit logs to build reports for each application or data source to provide auditors with proof of compliance. Instead, it enables the extraction of a holistic authorization picture per application.

Policies must be dynamic in nature to align with best cybersecurity practices such as Zero Trust. One key challenge is the controls shift amidst increasingly complex compliance regulations and the implementation of more applications. Orchestrated Authorization is dynamic authorization - it allows policies to become scalable to save time and enable business agility, while mitigating the risks associated with a siloed approach for each individual application. This business agility translates to faster implementation of new applications and platforms, seamless workflow across all business functions and departments, and growing potential for business advantages by having a strong security foundation that empowers the organization to focus on innovating the business.

While attributes are a key element of a dynamic policy, policy modelling is a specialized skill that necessitates a solid understanding of how attributes intersect and interact with one another. For example, a policy might say only full-time employees can access all information within an organization's HR system, while contractors can access limited information in the same database. However, if that contractor works closely with a different department, they would be given full access to that department's data. Access policies require expertise and transparency across all stakeholders, and must reflect the right kind of input. Every stakeholder type has a different set of roles and responsibilities that contribute to the larger goal of policy development and deployment in an ABAC environment.

Key Takeways

- **Policy attributes can differ** based on the simplicity or complexity of structural factors within an organization.
- In an attribute-based access control environment (ABAC), **attributes make a policy dynamic** as they are the elements that are modified to determine the right access path across an organization.
- **Dynamic attributes allow policies to become scalable** to save time and enable business agility by eliminating the need to build policies from scratch.
- **Policy modelling is a specialized skill** that necessitates a solid understanding of how attributes intersect and interact with one another.

Key stakeholders in policy development

While CISOs hold full accountability for policy deployment, identifying the right stakeholders for the policy authoring process is critical to determining the full scope of an organization's policies. Each team of stakeholders manages the application side for policy deployment, and drives business needs forward.

Organizations have varying needs, which means policy development requires multiple roles. These stakeholders can be categorized into three category types, each with a specific role.

Development stakeholders supervise the development of the apps and platforms used across the company, and must ensure these authorization requirements are built into their projects. Policy authoring typically resides in their role, as they understand the implementation of access requirements that avoids bogging down the authorization engine issuing a permit/deny decision. They recognize how to align policies with the holistic strategy outlined by the CISO and are responsible for simulating these policies while identifying and fixing gaps in real-time across each application prior to deployment.

Business management stakeholders such as finance and human resources teams oversee key functions and are able to determine who in their departments should have access to certain data and policies. Their role is to outline what the access path looks like for the employees under their departments, along with any cross-functional access paths. They are typically the source of the authorization requirements.

Executive stakeholders, including CISOs and/or identity leaders, are ultimately responsible for providing the direction as to how these policies contribute to corporate cyber initiatives with their broad view of the organization's overall security stance. Their role primarily focuses on ensuring adherence to regulatory compliance, with the CISO involved in the first stage of policy modelling.

Key stakeholders often work in tandem with one another to ensure policies remain effective and efficient, as it involves an ongoing review of these policies, especially when they have emerged from rigid and outdated legacy policies to offer room for constant adaptation amid evolving security risks and regulations. Each stakeholder's roles and responsibilities leverage their particular expertise, enabling less time-consuming exchanges due to the critical involvement of stakeholders across business functions.

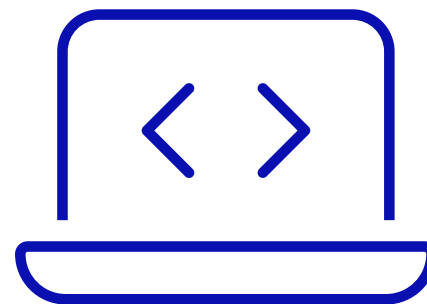
Key Takeways

- Development stakeholders are responsible for **policy authoring** as they oversee the apps and platforms used in an organization.
- Business management stakeholders are the **source of the authorization requirements**, determining who has access to what data.
- Executive stakeholders including CISOs and/or identity leaders provide the **direction for how policies adhere to regulatory compliance** and the organization's broader security initiatives.

Take the next steps

Learn how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

[Meet with our solution experts for a demo](#) of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:



[Blog articles](#)



[Press releases and announcements](#)



[Resources, solution briefs, and tools](#)



[Join us on LinkedIn](#)



[Subscribe to our LinkedIn Newsletter](#)



[Subscribe to our YouTube channel](#)

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: <https://linkedin.com/company/axiomatics>

Join us on YouTube: <https://youtube.com/@axiomatics>

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240