



WHITE PAPER

Accelerating Dynamic Authorization Through Cloud-native Development

Background

Historically, security and identity teams were viewed as policing application development, challenging that team's ability to deliver. As application development teams adopt cloud-native principles and understand the importance of a strong access control strategy, this presents opportunities for security and IAM teams to accelerate application development with the right guardrails in place. This starts with aligning on authorization strategies and DevOps processes during application development, especially when building microservice architectures and deploying API gateways.

Cloud-native authorization requires a centralized approach to access management, while decentralizing policy development. This modern approach is grounded in a dynamic, flexible method for access control. Modern authorization strategies such as dynamic authorization enable a holistic approach to authorization across multiple applications and resources within a cloud-native environment. As application development teams adopt this authorization strategy, there are opportunities to help developers accelerate development in the cloud.

Build a microservices architecture that can scale

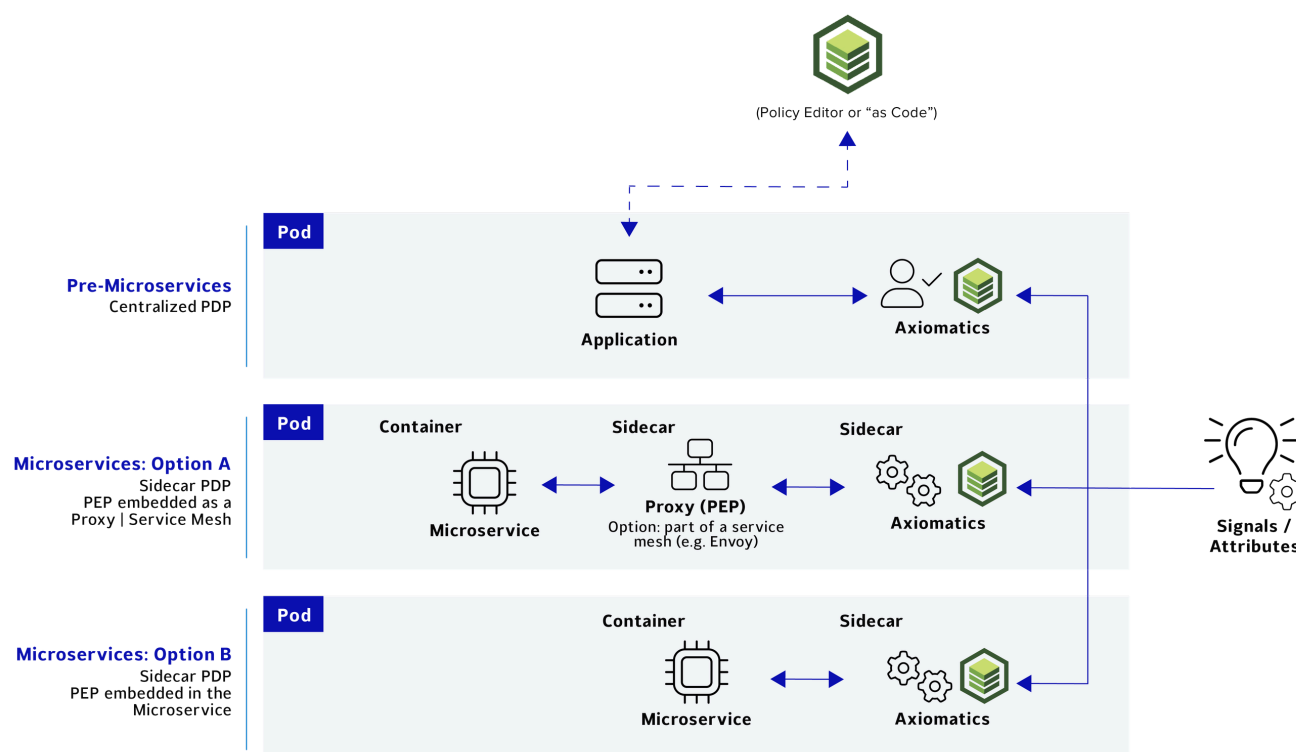
With business needs becoming more granular, developers are building cloud-native applications based on a microservices architecture. Microservices are the widely-adopted approach to application development in a cloud-native environment. With the ability to write each containerized service in a different language and run them on multiple services, it enables increased scalability and capabilities for applications.

Since a microservice application is developed as a collection of services, each service is self-contained with independent, separately-coded components that introduce greater complexity in a development pipeline. Each self-contained component has to ladder up to the cohesive application while being maintained and deployed individually, which can lead to security vulnerabilities across multiple attack surfaces. As such, the complex framework of a microservices architecture signals the need to approach authorization differently than a traditional monolithic architecture. Furthermore, with multiple endpoints to manage across individual services, microservices require a distributed policy approach to authorization that still considers multiple criteria for permission control.

To successfully apply authorization for microservices architectures, identity leaders must work with developers to outline the parameters that define the authorization policies for each microservice component. Since microservices mean a greater risk of operating within a siloed developer environment, they expose security vulnerabilities resulting from inconsistent authorization approaches. Engaging identity leaders at the start of the development process establishes the right guardrails for authorization throughout the development process by considering global policies and rules set by a central team. At each stage of use, authorization should function to safeguard granular parts of the services in a microservices application and foster secure information exchange and code deployment. This can be driven by the adaptability of modern authorization methods such as dynamic authorization.

When applying dynamic, context-aware access control to a microservices architecture, policies are built into microservices applications through multiple policy enforcement points (PEPs) that make decisions about whether access should be permitted or denied. While these PEPs can be integrated in a variety of ways, they are dependent on the centralized management of the attributes that inform the policies.

PEPs should be compatible with the environment they are operating within - in this case, a cloud-native environment. One method is implementing the PEP through a proxy, operating within a service mesh such as Envoy that facilitates internal communication between services in a microservices application. This can be coded either through a sidecar for each service, or creating a more centralized service at the node or cluster level. Another method is embedding the policy enforcement through a sidecar within the microservices application itself.



When firming up a cloud-native authorization strategy, adhering to modern access control frameworks, including Zero Trust, should be considered for a microservices architecture - especially given the need to secure discrete components. The PEPs must be founded on the attributes that exist within a central repository at the enterprise organization. These attributes should align for the access request to be granted. Whether it's an interaction between applications or an access request from a user, PEPs must repeatedly validate permissions as defined by modern security approaches (including Zero Trust) and safeguard microservices across all levels of access.

Key takeaways

- The granularity of a microservices architecture in a cloud-native environment necessitates a **fine-grained, unified approach to authorization**.
- Authorization policies are built into multiple enforcement points using a **sidecar method that enables the policy decision-making process for each individual service**.
- **API authorization is a key consideration in a microservices architecture** as it operates based on pre-coded rules and conditions.
- Each policy enforcement point should adhere to Zero Trust principles by **leveraging a stateless policy decision point that continually validates permissions based on real-time context**.

Opportunity: Strengthen the shift-left movement

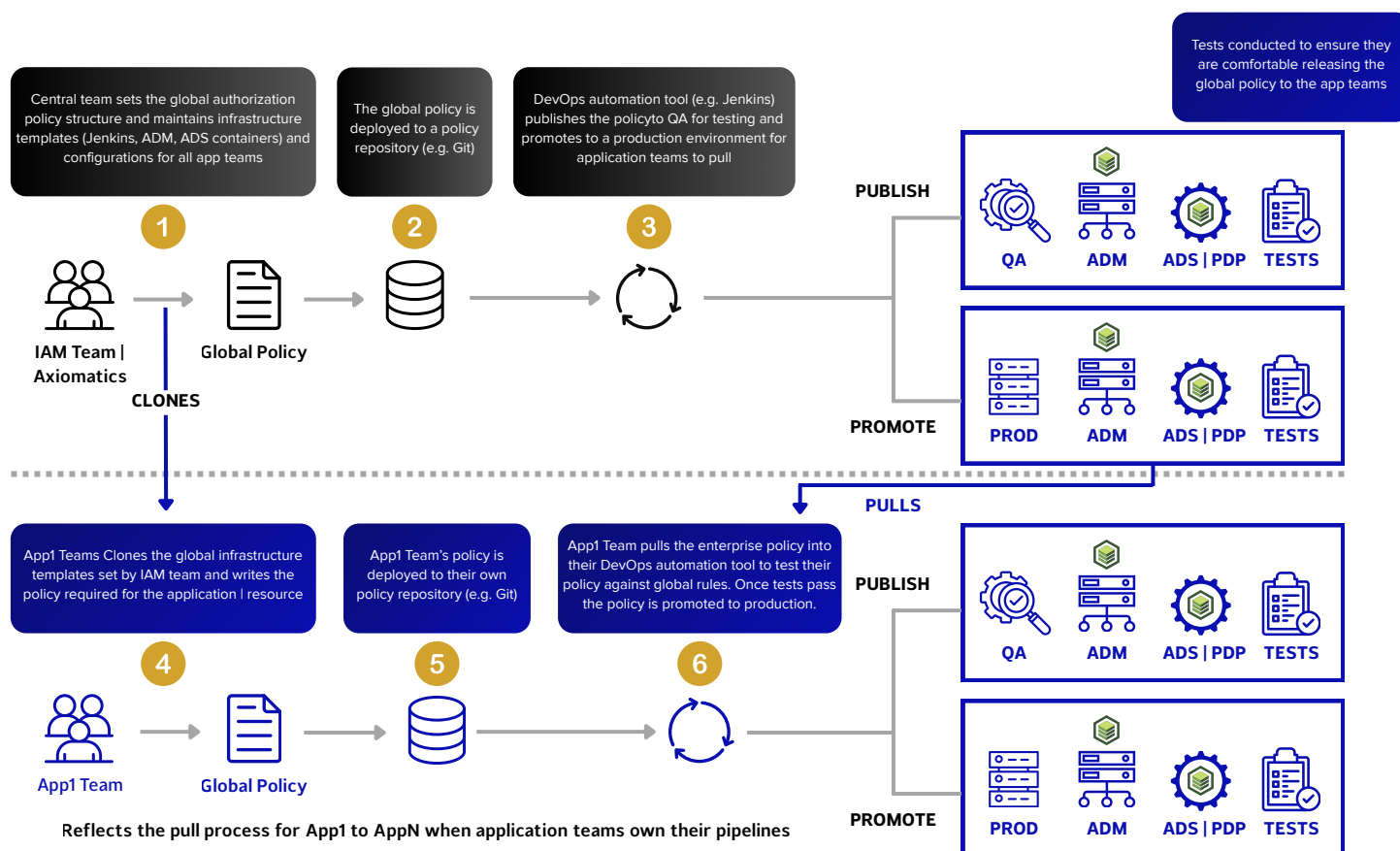
The practice of shift-left testing has increasingly become part of the DevOps process, as it focuses on identifying issues early in the development cycle. Shift-left testing is founded on the premise of testing early and often, which is a contrast to previous approaches to testing that were executed in the latter half of application development - including authorization testing. While shifting left is not a new concept, the broad adoption of DevOps forces enterprises to ensure that as DevOps momentum grows, they put the right checks in place to prevent broken continuous integration and continuous deployment (CI/CD) pipelines that risk production defects.

As part of dynamic authorization, IAM and security teams consider how to help developers automate the process of testing and deploying authorization policies within their CI/CD pipelines from staging to production. To drive shift-left security testing, developers should have the tools to incorporate authorization policies early in the development cycle using policy-as-code.

Policy-as-code automates policy deployment through authorization platforms, enforcing policies related to the authorization of a service. As-code platforms can accelerate the policy-as-code approach across applications by using language frameworks such as Abbreviated Language for Authorization (ALFA) and Open Policy Agent (OPA).

For example, with pre-packaged test frameworks in ALFA, security and IAM teams can remove the task for developers to have to create their own test frameworks and automated processes. In return, this changes the role of IAM and security teams from policing to enabling developers to adopt a shift-left culture.

Policy-as-Code distributed pull architecture



With multiple PEPs in cloud-native applications, policies built on dynamic authorization should be integrated with CI tools and testing frameworks for regression testing. CI tools enable developers to push out test scripts in real-time based on pre-defined triggers and perform automated tests based on integration. Using a dynamic authorization approach can be applied to denying test scripts access to production services in order to avoid accidental deployment based on specific attributes within the test script itself.

Ultimately, a shift-left approach must work in tandem with an adaptable authorization framework that enables the automated identification of policy issues as early as possible. Since dynamic authorization supports an attribute-based access control (ABAC) strategy, Development teams can implement access control policies with the confidence they'll be dynamic and respond to contextually-based decisions, not only enabling teams to shift left, but strengthening the delivery of a Zero Trust strategy.

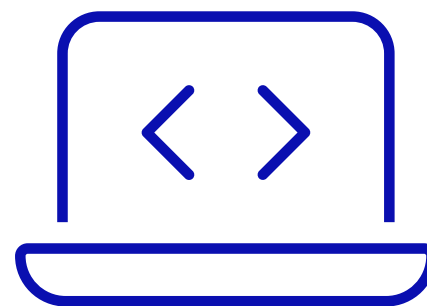
Key takeaways

- Encouraging a **shift-left culture can accelerate application development** instead of being perceived as a roadblock.
- **Shift-left testing requires the automation of security testing** throughout the development lifecycle adhering to a CI/CD pipeline, which includes authorization.
- Leveraging policy-as-code platforms equips developers with the ability to test and adapt authorization policies by **separating authorization from the cloud-native application**.
- To manage multiple policy enforcement points (PEPs), policies should be **integrated with CI tools and testing frameworks that enable developers to deploy test scripts in real-time**.

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