EXECUTIVE BRIEF

Making the shift to **Orchestrated Authorization**

AXIOMATICS

Abstract

Since the dawn of application development, organizations have attempted to implement authorization policies across application and data sources with varying degrees of effectiveness. Without a standardized approach to authorization, organizations will simply default to an **isolated authorization** strategy.

What is isolated authorization? Well, it's the way authorization has traditionally been done, with code and policies built into individual applications without any connection both to other applications or to a governing body of standards set by the organization. This approach is fraught with unnecessary complexity and ineffective design which can create additional attack surfaces and increase risk. This is further exasperated when you consider that the adoption of the cloud and microservices, application development has shifted from years to weeks. As a result, isolated authorization does not scale and leaves organizations exposed to cybersecurity risks while being unable to meet regulatory compliance requirements.

The only way to defeat isolated authorization is to leverage a more secure, scalable and easy-to-use alternative – **Orchestrated Authorization.** This executive brief will explain how Orchestrated Authorization provides the necessary tools to quickly build dynamic and fine-grained access control (FGAC) policies that meet the demands of modern security strategies including Zero Trust, and do so at the current pace of innovation. Organizations that can keep up with this new pace will thrive and be able to adapt in the new world, while others that struggle will be left behind.

"Isolated and ad-hoc does not scale. Become more secure with orchestrated and ongoing authorization."

The shift in scale

The undeniable change facing organizations today is that the adoption of cloud and microservices has led to them now dealing with hundreds of applications to serve their needs. Add to this equation the maturity of cybersecurity doctrines such as Zero Trust that require the continuous verification of access across **all layers of the application** (e.g. front-end pages, APIs, database) based on contextual attributes that change all the time (e.g. where, when who, what, how). Despite these two factors, the business and its users expect, if not demand, millisecond response times for authorization decisions. Manually managing authorization requirements at such a scale is near impossible, so the majority of organizations default to doing the best they can with what they have. This means control over which users are authorized and what they can do with these applications. as well as data sources lacks any centralized or consistent control. Ultimately, this represents a high degree of risk in terms of what can happen should information be exposed or malicious action occur.

Isolated and ad-hoc

Imagine trying to get every employee at a 1000-person company to save all their files with a specific naming convention. Some people will follow it, some will try to follow it but make mistakes, and some will just not even care. Now imagine instead of naming files, we're talking about writing authorization policies for any new application or data source added to the organization on an isolated, ad-hoc basis. In the end, due to a mixture of overprotection and apathy along with errors, you're not going to have consistent protection for your organization's applications and data sources. Additionally, trying to implement and enforce any sort of overarching policies is going to be almost impossible with this approach. Isolated authorization does not scale to the demands of an enterprise and complex regulations and audit requirements.

Orchestrated and ongoing

To overcome isolated authorization (which is already the reality at most organizations), identity and security leaders must offer developers and solution architects an easy-to-use alternative that is more secure and scalable – **Orchestrated Authorization**. This approach provides developers with the tools they need to quickly build dynamic and fine-grained access control policies that meet the demands of modern security strategies such as Zero Trust or identity-first security. Of equal importance, Orchestrated Authorization provides the business with an easy-to-use experience for developing the demanding policies they require to secure authorization at layers of the application. With silos broken down, central to this approach is a conductor who may serve as the CISO or independent identity leader in the organization. With an overarching view of policies, identity and security leaders possess the ability to execute on a strategy that offers both the speed and continuous control their cybersecurity program requires to protect their data. Orchestrated Authorization enables them to employ dynamic policies that take into account multiple attributes from multiple sources (e.g. who, what, when, where, why, how) to determine what a user should have access to and is authorized to do. Moving from the siloed, ad-hoc approach of isolated authorization to an orchestrated authorization strategy is akin to the difference between your grandparent's music collection of vinyl records versus a millennial's virtual digital music service app where they can find virtually any music ever recorded.

AXIOMATICS

What do organizations need to shift to Orchestrated Authorization?

The whole point of moving to Orchestrated Authorization is to simplify the process at scale and employ a centralized policy engine. At the core of the approach, there are three key requirements:

Translate business logic into authorization policies that reflect a Zero Trust framework

Why this matters

It moves the organization from the ad-hoc, "good enough" default authorization strategy made up of inconsistent policies. Instead, the organization elevates the maturity level of their cybersecurity stance with the ability to apply continuous Zero Trust enforcement to "always validate." This increases their security posture and lowers risk.

Apply dynamic authorization to newly built/acquired applications with minimal effort by internal developers

Why this matters

It removes the need for the organization to rebuild authorization policies from scratch for every new application added and allows them instead to leverage a "one to many" approach. This means a policy can be applied across multiple applications and easily changed later as needed. This saves time and enables business agility.

Provide a 'single source of truth' to easily show an auditor who can access an application and under what conditions

Why this matters

It eliminates the need for manual collection of audit logs to build reports for each application or data source to provide auditors with proof of compliance. Instead, this automates the on-demand extraction of a complete authorization picture per application, centralizing visibility and helping to ensure compliance via a standardized, transparent view.

The Bottom Line

Whether or not your organization adopts an Orchestrated Authorization strategy is not the question. The reality is, your team is already attempting to achieve authorization today. At issue is the manner in which they are addressing it. Do you want your team to continue to default to an isolated, ad-hoc approach, dealing with each application individually and continually writing separate policies? Or would you rather provide them with the necessary tools they need to leverage Orchestrated Authorization; enabling them to address the new shift in scale in a manner that increases your organization's cybersecurity posture, saves you time and provides you with centralized visibility?

If you're ready to explore the latter otion, we're here to help.