



WHITE PAPER

Key Considerations: Why Maturity is Integral to Driving Authorization Strategies Forward

Background

Large-scale change is challenging for organizations, especially when transitioning from legacy systems and processes to newer and more efficient methods. While navigating change can be tough, a phased approach fosters a smoother transition for people across all departments, and in some cases, across regions. This approach is particularly important in cybersecurity.

Traditionally, organizations treat cybersecurity initiatives with a sense of urgency as a short-term response to increased security threats or as an aftermath following security breaches. To effectively plan an authorization strategy and apply it across the business, a long-term outlook is required. This is where maturity comes in.

A maturity-based approach to cybersecurity allows all aspects of the business to be carefully considered throughout the development of an authorization strategy. It ensures that there are less gaps during the implementation process by addressing challenges early.

The following captures key considerations your organization should review to understand how maturity plays a role in driving the shift to a dynamic authorization strategy.

An overview of authorization maturity policy

The notion of a “right” approach to access control has historically been a point of contention in the security market. While broader conversations generally lean towards a dynamic authorization strategy founded on a Zero Trust architecture, there are different methods of deploying this strategy depending on the structure of an organization.

One approach is to build a strategy based on an orchestrated authorization framework, which equips organizations with the tools to drive dynamic authorization forward while enabling a secure and scalable access control process. Dynamic authorization centralizes authorization requirements to a unified source and applies a Zero Trust framework that consistently validates permissions for all users, resulting in seamless authorization policies.

Much like accumulating wisdom with age, organizations need to mature and reach a certain stage in their authorization journey – this is their market maturity. Despite the urgency in enhancing security protocols, it is more effective to manage security transitions in phases with clear goals that allow challenges to be identified ahead of wide-scale implementation. This is mitigated by the fact that some areas of security including identity and access management (IAM) have seen significant maturation in recent years, while others are still emerging.

Once organizations have a foundation for dynamic authorization, security and information teams need to follow a phased methodology for implementing new initiatives based on an authorization maturity model. While there are different maturity models for executing authorization strategies, one involves a three-stage process – crawl, walk, run. Regardless of the maturity model being used, the goal is to prove value to support broader adoption. Maturity models prepare the organization for short-term and long-term success, but the actual scope of each stage can vary based on where an organization is in their maturity within dynamic authorization. Ultimately, deploying authorization initiatives using a maturity-based approach ensures alignment across the organization.

Key Takeways

- Generally, the security market agrees on the value of dynamic authorization anchored in Zero Trust.
- The most productive way to shift to dynamic authorization is identifying organizations' market maturity by examining current access control initiatives and understanding their approach to security.
- Once organizations are at a later stage in their market maturity with a foundation for dynamic authorization, they can demonstrate the value of a dynamic authorization strategy by applying a phased maturity model.



Identifying market maturity

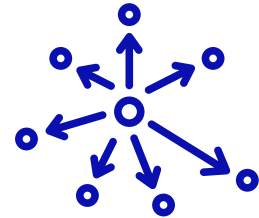
An organization's market maturity is defined by their place in the transition from static authorization to dynamic authorization. Market maturity differs from dynamic authorization maturity, as it includes organizations that have not adopted a dynamic approach to authorization.

Before an organization can begin deploying an authorization strategy, they must identify their position in embracing dynamic authorization based on the main driver behind their cybersecurity strategy. For many organizations, Zero Trust is the driving reference architecture behind their modern cyber security strategy. Regardless of the reference architecture, a sound cybersecurity strategy starts by ensuring policy decisions have the right context for access controls. Context can be derived from a number of sources, but the most important is having alignment on who is trying to access a particular resource. If organizations lack the ability to surface contextual attributes (e.g. identity, roles) then they may not be ready to embark on a dynamic authorization strategy.

There are numerous factors that contribute to authorization challenges, including how an organization is set up, the capacity of its security and IT teams, obtaining executive buy-in to a new authorization strategy, and even compatibility with legacy systems. Tackling these challenges begins with looking at the organization through a wider lens - determining its market maturity.

Market maturity is categorized by four levels of access: fragmented, unified, contextual and adaptive. A standard authorization journey is the graduation from fragmented to adaptive, representing the improvement of an organization's security measures.

Fragmented identities occur under static authorization, where there is no cloud integration and passwords are not managed on a single platform. This is characterized by identity sprawl, where a user's identity is split across isolated systems that leave information vulnerable to attackers rather than centralized to a directory. Since these systems are out of sync, security policies would be difficult to enforce.



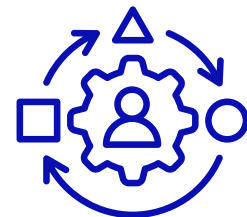
Unified identities solve the primary challenge of fragmented identities by generating more secure processes with multi-factor authentication and password access management tools. It offers a single sign-on for users across the organization. However, a unified identity strategy is limited to role-based access control (RBAC), which is a good place to start but does not enable the types of policies modern security strategies (e.g. Zero Trust) demand.



Contextual access represent the transition to dynamic authorization, with context-based access policies based on the type of user accessing the data. It accounts for the dynamic context of organizations, providing access based on multiple user attributes. While this is a key improvement, it may still lead to security loopholes without constant permission validation.



Adaptive access take context-based policies and upgrade them to risk-based policies, enabling more secure and frictionless access. While multiple user attributes are built into this access level, these identities are validated on a regular basis. Security and IT departments need to mature to an adaptive access approach prior to thinking about dynamic authorization maturity, which is defined by continuous authentication and risk-based policies and founded on a Zero Trust strategy.



Organizations need to examine where they are in their authorization initiatives and map out the path to adaptive access before even thinking about authorization deployment. Otherwise, businesses run the risk of encountering challenges that delay the transition, such as addressing individual risks for each application rather than applying risk-based policies across all applications.

Key Takeaways

- Organizations must determine their market maturity in the journey to dynamic authorization prior to deploying authorization initiatives.
- There are four levels of access that define an organization's place in their authorization journey: fragmented, unified, contextual and adaptive.
- As a best practice, organizations should be at the adaptive access level with a dynamic authorization strategy they can align to ahead of deployment.

Authorization maturity is an integral consideration in the deployment of authorization initiatives across an organization, reflecting best practices for change management. With over 20 years of experience working with Fortune 500 organizations, Axiomatics' approach to authorization reflects the evolving needs of the business landscape.

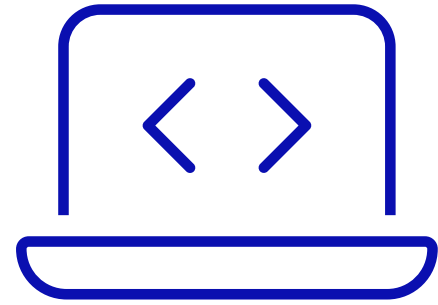
We welcome the opportunity to connect and provide you with a perspective on authorization maturity and how this can be operationalized across all areas of your business.

Reach out to Axiomatics for a consultation on where your organization's maturity stands in the authorization market.

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