AXIOMATICS

You asked, we answered:

Tackling popular customer questions on authorization

Authorization, while a hot topic, is still a difficult one for many organizations to wrap their minds around. As the Axiomatics team talks with customers and prospective customers worldwide, a few common questions inevitably arise. In this piece we'll take aim at these questions, offering guidance on why authorization makes sense as a priority and can, in fact, enable other organizational imperatives including Zero Trust and compliance initiatives.

Question #1: We're already leveraging role-based access control (RBAC) through an authentication or identity governance administration (IGA) tool. Why would we need an authorization tool?

Role-based access control (RBAC) has been around for a long time, which is why it is so well engrained in many organizations. Many Axiomatics customers also use an RBAC tool. They purchased an attribute-based access control (ABAC) solution from Axiomatics because they found that establishing, implementing and updating roles became a very labor-intensive process.

For organizations leaning on RBAC through another solution, they often find their IT departments become inundated with individual or "one-off" requests to create a new role for someone. With that framework, it doesn't take long to be buried under an avalanche of roles, making it difficult to have a clear understanding of what roles have been created and how the organization is achieving compliance with various regulations.

The purpose of an ABAC solution is to add to existing IGA and/or authentication solutions, delivering assurance that even after someone is authenticated by the organization, proving they are who they say they are, they only have access to the data and processes they require – nothing more, nothing less. Examining attributes

(location, time of access request, type of request, device making request, etc.) also enables an organization to proactively determine if the access request is potentially concerning. For example, if an employee who consistently accesses an asset with sensitive information via their laptop in the morning all of a sudden makes a request after midnight from their mobile phone, even if their authentication was verified, it's fair to assume this request poses additional risk to the organization and may require additional verification.

For more insight on authentication versus authorization, check out this white paper.

Authentication and IGA are incredibly valuable solutions for every organization. Authorization enables those investments to do more, strengthening a business' overall security stance.

Question #2: We have a privileged access management solution. Won't that cover authorization?

Organizations that have a privileged access management (PAM) solution understand the importance of authorization and have invested to protect some of their most important applications and resources. Most PAM solutions are quite powerful and are specifically designed for that organization's administrators to use, because managing a PAM solution does not scale - it is designed for privileged users, which is a small group that usually doesn't experience rapid or exponential growth.

And therein lies the problem. As new threats and compliance requirements emerge, many organizations wish the capabilities they love in their PAM solution would scale across the rest of their users and even customers. This is where ABAC can bridge the gap. Using a dynamic ABAC solution, organizations can configure and leverage simple or complex policies that can be applied to all applications in an easy-to-manage manner. The ability to write once and push out as much as you need for users, partners or even customers to leverage means lower risk and faster time-to-value.

Even so, PAM solutions aren't without their own issues. A recent survey from the Ponemon Institute found issues with access rights. Critically, more than a third of respondents indicated they had access to data not required for their job. In addition, 36 percent of those said they did not need privileged access to do their jobs... but had it anyway, as either everyone at their job level had privileged access (whether required or not) or their organization did not revoke rights after their role(s) changed. Ensuring the right users have the right access is a central way in which ABAC can extend PAM capabilities.

Another advantage to an ABAC solution is around troubleshooting database queries. While privileged users likely need to access different systems to troubleshoot queries to the database, they likely do not need to see any of the sensitive data contained within these databases. This is why many organizations using both PAM and

Question #3: Why should authorization be a priority for us?

ABAC solutions have to leverage functions like session recording or key-stroke logging to clarify exactly in what way privileged users interacted with the database. This means privileged users can troubleshoot and fix issues, but not be exposed to the sensitive data in the first place.

This is a question on the minds of a lot of security or identity leaders and many business users, too. But as enterprise environments become more complex (and, frankly, as the world becomes more complex), it is more critical than ever to ensure trust across all activities while concurrently providing an efficient experience to user clients and employees. It's for that reason authorization becomes a worthy investment.

There are always conflicting priorities within an organization. After all, the list of organizational imperatives is a long one, both within and without security. But authorization is an area that for too many organizations only becomes critical after there's a serious breach or when an inadequate customer experience comes to light. At that point, prioritizing authorization is too little, too late. In fact, with Zero Trust becoming a standard for any organization that values security, authorization can help make these deployments more straightforward and more effective. This is because it provides better visibility of what policies are in place, who can access what data and processes, and when and how they should have said access.

Question #4: Our development team says they currently add authorization capabilities via an internal process. Why should we move away from this practice?

Developers who add authorization as a dedicated part of the application development process clearly recognize its value, which is great! There are a few things to consider before constraining a highly-skilled development team to with additional duties:

1. How much is their time worth? Should developers be creating a customer authorization engine from scratch, or should they be focused on initiatives directly tied to generating revenue?
2. Will a custom-built authorization engine be scalable and repeatable across all applications and/or be easily managed?
3. Will authorization isolated in each application require separate coding that must be updated on an application-by-application basis whenever there's a new requirement the organization must adhere to?

These are difficult questions for many organizations to answer. For those that opt for authorization solutions, they understand developer time is incredibly valuable and should be focused on bringing revenue-generating

applications to market. To make the best use of their skills and time, authorization should be managed via a centralized, externalized platform. Additionally, Axiomatics' ALFA language provides developers with a simple way to write authorization policies in a language akin to software development languages like Java or Python. Leveraging ALFA enables simplified collaboration between business and IT by facilitating and automating authorization policy writing and management, making it an easy alternative to writing in code. Both easy to maintain and simple to update, ALFA enables developer insight into authorization that is centralized, making authorization both scalable and repeatable across the organization.

Question #5:
This feels like a significant undertaking. We're more focused on Zero Trust as a priority, so how can I justify adding authorization right now?

Incredibly glad to see more organizations are embracing Zero Trust as a core security tent. At its core, Zero Trust means no users or devices are to be trusted without continuous verification.

Authorization delivered through ABAC actually enables a Zero Trust model and deployment. Developing centralized policies that are informed by dynamic attributes means policies become dynamic and take into account multiple attributes from as many sources of data as possible to determine what a user is authorized to do. This is why NIST emphasized that authorization (as well as authentication) was a core component in creating access rules that are as granular as possible, creating a 'least privileged access' model. In short, authorization is a core piece of your Zero Trust initiative, not a project above and beyond that endeavor.

Learn more about authorization as key to Zero Trust in this video.

About Axiomatics

Axiomatics 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's Orchestrated Authorization strategy 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. To learn more, please visit our website or follow us on LinkedIn , Twitter , and YouTube.

Learn more at **axiomatics.com**
webinfo@axiomatics.com
US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240

AXIOMATICS