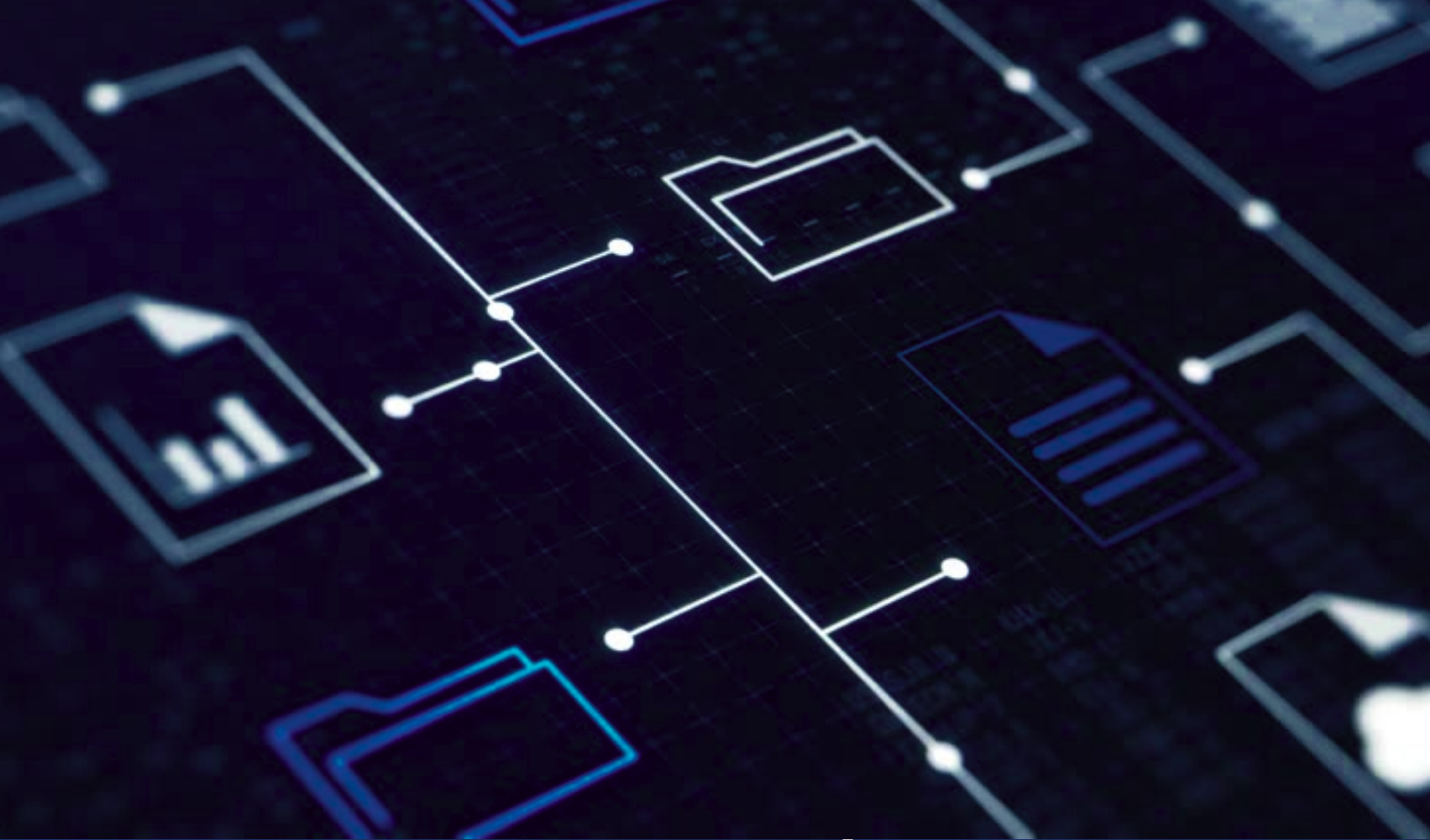




SOLUTION OVERVIEW

Contextual Authorization Query: Simplifying entitlement reviews and data filtering

With an increasing number of global regulations, identity teams face many challenges, including answering detailed questions about user access to sensitive information. While an access review or recertification process addresses these questions, the result is most useful only at the time at which the review is completed.

Contextual Authorization Query (CAQ) offers a multi-dimensional view to access questions, serving as a powerful solution to streamline [entitlement](#) reviews and enhance data filtering in applications.

Why does this matter? Let's explore.

Understanding Contextual Authorization Query

Contextual Authorization Query is a reverse query tool that retrieves authorization information from the policy. It provides a list of conditions that describe who, what, when, where, why, and how information can be accessed in an application. For instance, you can ask questions like, "What can Michael eat on Friday?" to get specific authorization details.

Key use cases for CAQ

Entitlement reviews

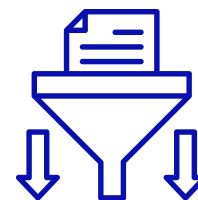
Organizations often need to know what resources and data an employee has access to or under what conditions a user can access sensitive information.



CAQ simplifies entitlement reviews by providing a comprehensive overview of user permissions and access conditions.

Data filtering

CAQ excels in scenarios where a user wants to access a dataset and only retrieve the data they are authorized to view.



By applying CAQ data filtering, applications can efficiently pull only the relevant records based on the user's permissions, reducing workload and ensuring compliance.

Simplifying entitlement reviews

Adopting a [policy-driven authorization](#) strategy enables organizations to apply principles of least privilege for every user accessing information across the application landscape. conditions.

The applications that adopt these policies will be leveraging various contextual attributes such as user properties, action type, environment attributes, and resource properties. CAQ simplifies entitlement reviews by providing a comprehensive view of access conditions.

When submitting an entitlement review request to CAQ, its response is "contextualized" by connecting to and/or providing relevant attributes to interrogate the authorization policy effectively. For example, specifying or connecting to the attribute source that contains the region and industry helps narrow down the results to specific access conditions. CAQ then generates two types of responses:

1

Simplified response:

A textual, readable output that highlights the key access conditions, making it easy for human auditors to review at a glance.

2

Raw expression

A nested syntax tree containing all the policy decision details, which can be consumed by entitlement applications for detailed access review reports.

Determining user permissions with CAQ

CAQ determines user permissions by evaluating the authorization policy against the provided context. It considers factors such as user attributes, resource properties, and environmental conditions to generate a comprehensive list of access conditions.

For instance, in the purchase order application, CAQ might determine that managers in the US region with specific training can delete records, while senior managers have broader access regardless of industry or region. It also identifies any additional conditions, such as users not being able to remove records they own.

Enhancing data filtering with CAQ

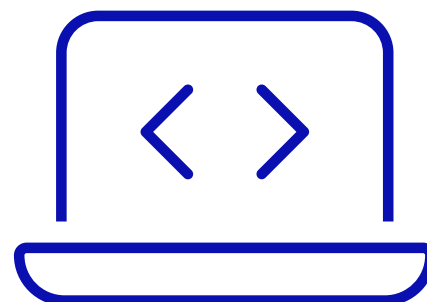
Let's consider a purchase order application where different users have varying levels of access. When a manager views the purchase orders, CAQ data filtering ensures that they only see the records they are authorized to view based on their role and region. On the other hand, an employee who is not a manager, can only view records where they are the order owner.

Behind the scenes, CAQ efficiently queries the authorization policy and the purchase order database, retrieving only the records that each user is allowed to access. This approach significantly reduces the workload compared to traditional [attribute-based access control \(ABAC\)](#) systems that review each record line by line.

See Contextual Authorization Query in action

By providing a comprehensive view of access conditions and efficiently querying authorization policies, CAQ simplifies compliance efforts and enhances data security. With its ability to streamline entitlement reviews and optimize data filtering, CAQ proves to be an invaluable tool in the realm of [fine-grained access control](#).

[Request a demo](#) with our team to see for yourself how CAQ revolutionizes the way organizations handle entitlement reviews and data filtering.



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