FACT SHEET

Four Ways Insurance Companies Can Leverage Authorization

Even though the insurance industry is a part of the highly regulated financial sector they are increasingly being targeted by cybercriminals. According to a recent report, insurance companies store a vast amount of Personal Identifiable Information (PII) in outdated systems, and they lack user training. Plus, they were slow to adopt a strong authentication strategy which led to nearly half (47%) of all breaches in the financial services sector affecting the insurance industry in 2022.

As a result, insurance companies are beginning to implement authorization solutions to protect customers' privacy and information through access control.

Here are four ways insurance companies can leverage authorization.

1 Reduce role explosion within international programs (IP)

When there are insurance contracts for international clients which have coverage spanning across multiple locations, each country should only have access to that country's relevant information. Along those lines, service hubs within that country should only have access to all relevant contract information for that region and the producing office will have access to the whole contract.

For the IP to do this, they must issue a high number of different roles to provide entitlements for each country and broker that are a part of the overall organization structure. This is because each country must have a complete set of roles for all functions, multiply that by the number of countries and brokers therein, which creates a huge number of roles that need to be managed. This is known as role explosion and is common when using a role-based access control (RBAC) approach.

Attribute-based access control (ABAC) can limit the need for a high number of roles by using attributes and policies. By adding context, access decisions are made based not only on a user's role, but also by considering who or what that user is related to, what that user needs access to, where that user needs access from, when that user needs access, and how that user is accessing the requested information.

2 Add a fine-grained approach to delegate permissions

There are many cases where permissions may need to be delegated to other employees. This can be difficult as many identity solutions use an RBAC approach, which means the employee must be elevated temporarily in the system for them to have the same rights as the person they are covering for at work.

This is problematic as it is such a broad statement to give employee B the same permissions as employee A (who will be out of the office). You need to consider if employee A has access to special projects or contracts that the other employee shouldn't see. Perhaps employee A already has more entitlements that they have acquired over a long tenure that they should no longer even have. If you just do a broad stroke delegation of all the entitlements, employee B now has all of those unnecessary entitlements as well, which creates additional risk.

In this case, ABAC is an ideal situation as it provides a fine-grained approach. It enables you to ask specific questions such as,"What does employee B truly need access to?," and only delegate those specific entitlements. As a bonus, the ABAC approach checks policies at each access attempt which catches unnecessary entitlements any employee has acquired over time through entitlement creep.

3 Remove the burden of access policies in agile development and deployment

Authorization can be integrated into the (continuous integration and continuous delivery/continuous deployment) CI/CD journey across all agile release trains. When working on trains to add features into applications, authorization must be considered, even as implementing access policies can be an afterthought for developers.

However, in the case of a custom application, it can be hard to implement authorization as you likely have to go into the code to change the policies. Any code changes require regression and QA testing which can be quite time consuming. Relying on an external authorization tool means policy updates are integrated into the application without any code changes. This removes the burden on developers, limits testing requirements, and ensures the application remains secure.

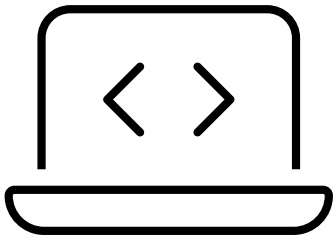
4 Use Zero Trust to protect assets

Traditional perimeter security paradigms are no longer sufficient to protect assets. It has outpaced the legacy security principles and architecture still in place in many agencies. This is a really bad place to be in terms of security.

ABAC as part of a Zero Trust strategy enables dynamic access to resources based on multiple attributes which can include the user, the device, location, behavior risk score, and so on. The policies that allow this can adjust access permissions dynamically. For example, it could be the right user, right device, but perhaps the user is not in the office so the policy enables access but with anonymized data. In this scenario, the employee can still do their job, but the data is still protected. Therefore, ABAC allows for a real-time response to changes in the trust level or to any threats detected.

Why Axiomatics

Axiomatics continues to provide its award-winning authorization platform to insurance companies worldwide. We provide a policy and attributed-based approach to access control that can be used at multiple layers including applications, APIs, and microservices.



See why so many financial institutions across the globe have used our authorization solutions.

Request a demo with one of our solution experts to see our award-winning offering in action.

Policy-based access control solutions for enterptise

Axiomatics has been solving the challenge of authorization for organizations since 2006. Their solution and proven approach simplifies the orchestration of fine-grained authorization to organization's applications, information, and processes via a central, dynamic, Zero Trust policy engine. This centralized approach removes the burden of coding and managing authorization functionality for each application separately while ensuring a consistent set of compliance and security policies are properly engaged across the organization.

For more information or to request a demo, please visit **axiomatics.com**.

About Axiomatics

Axiomatics is the originator and leading provider of runtime, fine-grained, dynamic authorization delivered with Attribute Based Access Control (ABAC) for applications, data, APIs, and microservices.

The world's largest enterprises and government agencies use the Axiomatics Dynamic Authorization Suite to enable digital transformation, share and safeguard sensitive information, meet compliance requirements and minimize data fraud. Our innovative solutions enable enterprises to share sensitive, valuable and regulated digital assets – but only to authorized users and in the right context.

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

AXIOMATICS