



WHITE PAPER

Build vs. Buy: Dynamic Authorization Solutions

Securing access control
while staying true to your
core business

When should you consider investing in dynamic authorization software versus building your own solution, in-house?

When evaluating the best approach to securing your APIs, applications, AI, and cloud, organizations are often caught in the decision of building a framework in-house vs. engaging a vendor to help. There are several key advantages to partnering with a vendor that specializes in fine-grained access control solutions rather than trying to build an equivalent solution using in-house resources.

Within this review, you'll find an assessment of the technological, price point, time-to-market, and ongoing maintenance and enhancement advantages of utilizing a dedicated security partner versus attempting to replicate a secure, scalable, and comprehensive solution in-house.

You want control over the project budget

The costs associated with building and maintaining a fine-grained access control solution may be one of the first and most logical reasons for a business to avoid choosing this option. Building a solution in-house may seem like a smart way to have full control over your budget, but in reality, unexpected costs are more likely to arise than if you went through a partner. Custom building and in-house maintenance is almost always going to be the more expensive endeavor.

For in-house solutions, pricing is rarely predictable. According to a McKinsey survey of IT executives, large IT projects run over budget 45% of the time, while delivering 56% less value than planned. The same study found that 17% of projects go so badly that they “threaten the very existence of the company.” These high-impact overruns, often referred to as “black swans,” see budget overruns of anywhere between 200 and 400% and can end in project abandonment.

“...large IT projects run over budget 45% of the time, while delivering 56% less value than planned. The same study found that 17% of projects go so badly that they ‘threaten the very existence of the company.’”



An [earlier study by the Harvard Business Review](#) found a similar result, where one out of every six large IT projects the researchers studied fell into this “black swan” category.

Depending on the maturity of your own development team, there are many steps to consider that may be involved in building your own solution:

- Research
- Staff acquisition
- Installation and configuration for POC environment
- Creation and configuration of policy-based access control infrastructure - information points, enforcement points, decision points
- Identification of attributes and their sources
- Policy lifecycle considerations: modeling, writing, testing, implementation
- Definition and execution of policy test plan
- Documentation of implementation and procedures
- QA
- Ongoing Support and Maintenance
- Compliance and Auditing

A dedicated security technology partner can offer a detailed and efficient installation and upkeep schedule that can save your organization money in the long run and therefore can make much more financial sense.

Your development team has better things to do

While the allure of a new challenge and the opportunity to build something may sound appealing to a development team, maintaining logic built into an application is costly and inefficient for upfront development and maintenance costs. Not to mention, it's not great for a developer's morale to be stuck writing and rewriting security code. The welcome challenge quickly becomes a tedious and repetitive chore.

If your engineering team is writing and maintaining custom code, this likely means they can't focus on core business projects that could be driving your business forward.



While the allure of a new challenge and the opportunity to build something may sound appealing to a development team, maintaining logic built into an application is costly and inefficient for upfront development and maintenance costs. Not to mention, it's not great for a developer's morale to be stuck writing and rewriting security code. The welcome challenge quickly becomes a tedious and repetitive chore.

With an access control solution such as dynamic authorization, it is possible to reuse access policies, meaning coding once and applying that code over the entire application ecosystem. This frees up your development team to focus on their key initiatives while eliminating the need to write custom code for every complex access requirement.

The modern software ecosystem has created a level of complexity that is increasingly hard to manage, and partnering with a security technology expert can help your organization keep pace with development without sacrificing security.

You don't have the time and internal resources to commit to a multi-year security project

Building your own policy decision engine and writing policies on your own takes a great deal of time and resources to successfully complete.

Development teams often don't have enough internal resources to secure every application, so they are picking and choosing customer-facing apps, while not securing other – possibly back-end – systems. The rate of software being developed is increasing and human skills cannot keep up to secure it. Right now businesses might only secure 5 – 10% of their applications.

As a dynamic authorization provider, we have taken on several large enterprise clients who began building in-house, only to abandon the project and start over with us. These companies took a loss on countless man hours, large IT “special project” budgets, and not to mention all the man hours responsible for getting that large budget approved.

A successful dynamic authorization implementation can set you up to proactively secure applications while your team is building them, instead of making security an afterthought.

A security technology expert has already solved your problems...and solved them well

If a problem has been adequately solved in a commercial product, why solve it again? Ask yourself and your development team: “Do I currently possess the resources and expertise to make the software better, or equally as good, than those solutions currently available?”

Security solution providers who are dedicated to providing authorization software are more focused. They have thought of issues that you won't because they have more resources and expertise to spend on thinking of those things. That means you'll have to deal with fewer bugs and issues with a credible third party than you would by building the software yourself.



What's your priority - to become a security company or to be a secure company?

Effective compliance and governance are important to your company

Software providers in general are well-versed in compliance rules, laws, and other regulatory requirements as part of their development process. This means they have developed, built, and refined their offerings to incorporate the functionality needed to address both the business/regulation side and from the technical side. In many instances, existing software could be able to meet a customer's compliance requirements, regardless of industry.

If you plan to change anything (or simply maintain)

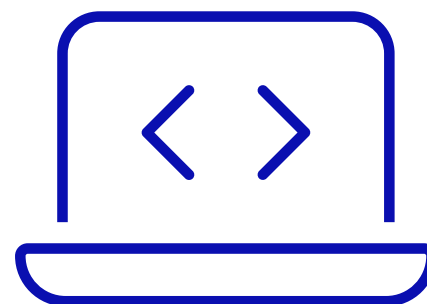
Your team is responsible for maintaining the custom solution, meaning that if it needs to change or the outside environment evolves, it will cost several development cycles to get back to normal. And that can only mean more of your team's time and more of your company's dollars.

You have to consider the secondary cost of ongoing support for a custom built solution which is essential for proper maintenance. It is common to see enterprises abandon their home built security system when the development has moved on. This leaves you with no ability to make changes required by business trends, regulations, or 3rd party integrations. The latter point is a notable consideration given that 3rd party external systems like CRM, ERP, payment gateways, etc. are constantly evolving.

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