SCALED ACCESS

WHITEPAPER

10 Reasons to Buy an Access Management Tool Rather Than Build

(It's not all about money, you know...)

Intro

When it comes to choosing whether to buy or build an access solution, the primary factor is usually cost. If it's cheaper to buy than build, surely you should buy.

You need to ask yourself:

- Do we need to hire additional expert developers?
- Can we properly estimate the budget and resources for building our own?
- What are the costs associated with maintaining our own independent access management tool?

Beyond costs and benefits, here are 10 additional reasons for choosing to buy over build:

1. Scope – Do you really understand the complexity of your ecosystem?

Can you plan out the full scope of your own access management tool?

It's often much more extensive than you think. Advanced access solutions take additional variables into account, such as:

- Confidential data, content and smart devices are shared by multiple users.
- Some users should hold privileged access.
- Users come and go.
- Relationships change.
- Data access should always be subject to consent.
- Privacy is key.

Advanced access management systems are tailored for these requirements and many others.

Custom-built features are also available. In fact, many platforms contain core features that were built based on customer feedback.

2. Expertise – Do you have the competency to build your own access management platform?

Are you prepared to train your developers in IAM standards like OAuth 2.0, OpenID Connect 1.0, UMA 2.0 and XACML, just for this project? Do you have the time?

IAM developer specialists are like gold dust. Throw in the ever-evolving IAM industry, and you're facing the reality of having to tiptoe around developers and keeping your inhouse IAM knowledge constantly up to date.

Buying an Access Management solution means buying domain expertise. No need to hire specialists or re-train your IT team. Instead, save time, money and resources.

> **Buying an access management solution means you're buying domain expertise.**

3. Security – Is it a good idea to hand your security over to a front-end junior developer that just *happens* to know the standards?

According to the Identity Management Institute report, 2019 was one of the worst years ever for data breaches; many of which could have been avoided with better access management[1]. The IMI named CapitalOne bank as one of the biggest hack-targets of 2019, compromising customer information dated back to 2005.

[1] https://www.identitymanagementinstitute.org/data-breaches-and-iam-trends/

Buy a proven access solution to secure your applications. You don't want to be listed in the IMI's next report.

> **Access management is an essential security microservice and it better be good.**
>
> **Otherwise, your whole platform is at risk.**

4. User Experience – Can your developer team build a tool that provides the best possible user experience?

Let's get one thing straight: IAM is not *just* about security. It's also about creating the best possible user experience.

Why display resources your users can't access? Although the user flow may run smoothly from an IAM perspective, that may not be the case from the user point-of-view.

> **Access management providers are not only focused on keeping the bad guys out, they also focus on keeping the good guys - your customers - inside and active.**

5. Maintenance – Keep in mind that your access management tool requires constant maintenance?

Every access management tool requires proper maintenance. Libraries and frameworks are renewed on a regular basis. Requirements change. New features are needed. Outdated code can develop bugs or become unsupported.

Professional IAM developers are expensive to retain. And relying on your regular IT staff‘s competence is not an option.

Access management providers have dedicated support and DevOps teams to maintain and optimize their platform by releasing new code and new features.

Outsourcing will bring you keep your mind at ease. Access security will no longer be your problem. Let domain experts handle it.

6. Time To Market – How much time will it take to develop your own access management tool?

Will building your own solution delay bringing your product to the market?

IAM is a specialist domain of expertise. Building your own tools requires you to obtain deep inside knowledge before you can even begin to build. And that’s besides the unexpected delays you’re likely to encounter during the build.

Externalized access management is readily available. It gives you everything you need, so you can enter the market at your best convenience.

7. Focusing On Strategic Issues – Do you really want your best developers developing an access management tool?

Do you specialize in IAM solutions?

The answer is no.

Whether you're in Financial Services, Healthcare, Media or Consumer IoT, you need to make sure that your best developers are working on whatever it is that makes your business stand out.

> **Focus on what you're good at and leave authorization to the experts.**

8. Agility – How quickly can you adapt when you need to make changes to your security policy?

Access management platforms allow you to externalize your authorization so that you can change your access policy without needing to change your applications. This enables new security policies to be easily deployed and enforced across all your applications.

Let's say your customer signed up for a free 30-day trial and you want to extend it to 60 days, you can simply update the access policy in the access management tool without changing your actual applications.

Simple.

9. Innovation – You don't want to be left behind as IAM evolves.

Access management providers constantly improve their platforms, adding new features to help you discover new business opportunities.

Blockchain and Real-time Anomaly Alerting are just two of the trends poised to make an impact in the IAM industry. With all this already done for you by the provider, you can benefit without any additional strain.

Stay ahead of the curve.

10. Standards (Interoperability) – Are you sure you can adhere to the industry standards?

Are you aware of the prerequisites needed to satisfy those standards?

Are you confident you won't accidentally descope vital features?

Access Management solutions should be fully interoperable and compliant with IAM industry standards. Using OAuth 2.0 and OpenID Connect 1.0 standards means users can interact with your services, even if they come from a different platform.

On a build project you cannot focus on satisfying these standards. Don't compromise on standard specifications. Buy.

In Summary

It's clear to see that the benefits of buying an access management tool significantly outweighs the reasons to build your own. With superior know-how, state-of-the-art security, an improved user experience and much more, access management providers will take care of authorization for you so that your company can focus on your own areas of expertise.

So, when you're faced with the choice of whether to buy or build, the answer is obvious. Buy.