



**WHITEPAPER**

# 10 Reasons to Buy an Access Management Tool Rather Than Build (It's not all about money, you know...)

**10**

## 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've got to ask yourself:

- Do we need to hire expensive specialist developers we don't currently have?
- If we build it, are we sure we can properly estimate the budget and resources for it?
- Will it be expensive to maintain our own built access management tool?

However, there are other key factors besides financial ones.

Here are the top 10 *non-economical* reasons to buy over build:

### **1. Scope – Do you actually understand the complexity of your ecosystem?**

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

It's often much more extensive than you think. Advanced access solutions foresee that:

- Multiple users share the same content, confidential data and smart devices.
- Some users should be able to see or do more.
- Users come and go.
- Relationships between users change.
- The access and use of personal data should always be subject to consent.
- Privacy is a key.

Advanced access management systems are tailored to answer these challenges and more.

They contain features you may not have thought about - like Token Introspection or Token Revocation. Even if you need custom-built features, they can usually do that. In fact, many platforms actually contain core features built based on customer feedback.

## **2. Expertise – Do you really have the expertise needed to build your own access management platform?**

Are you prepared for your developers to spend time learning IAM standards like OAuth 2.0, OpenID Connect 2.0, UMA 2.0 and XACML, just for this project?

It's common knowledge that IAM developer specialists are like gold dust. Pair that with an ever-evolving IAM industry, and you face the challenge of tiptoeing around developers and having to constantly update your inhouse IAM knowledge.

However, buying an access management solution means you're buying domain expertise. No need to hire specialists or completely retrain your IT team. Save time, money and resources.

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

## **3. Security – Do you really want to hang your security on a front-end junior developer that happens to know the standards?**

The Identity Management Institute reports that 2019 was one of the worst years ever for data breaches; many of which could have been avoided with better access management<sup>1</sup>. The IMI named CapitalOne bank as one of the biggest names to be hacked in 2019, compromising customer information dated back to 2005. Don't let that be you...

**Access management is a critical security microservice to your platform and it better be good. Otherwise, your whole platform is at risk.**

#### **4. User Experience – Can your developers 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 from an IAM perspective the user flow may be correct, from a user experience point-of-view it's a bad user flow.

**Access management providers are not only focused on keeping the bad guys out, they also focus on keeping the good guys (customers) in and active.**

---

<sup>1</sup> <https://www.identitymanagementinstitute.org/data-breaches-and-iam-trends/>

## **5. Maintenance** – Have you factored in that your access management tool will require constant maintenance?

Really want to keep those pricey specialist IAM developers on your payroll?

How about relying on your regular IT staff to do what's necessary to maintain your own tool?

Every access management tool requires maintenance. New libraries and frameworks are regularly released. Requirements change. New features are needed. Old code develops bugs or may no longer be supported.

But, that's why access management providers have a dedicated support and DevOps team to maintain and optimise their platform with updated code and new features.

Outsourcing brings peace of mind. It's not your problem anymore. Let the experts deal with it.

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

Will building your own tool delay you taking your products and services to market?

IAM is a very specialist domain. Building your own tool really requires inside knowledge before the build even starts. That's not to mention any unexpected delays that crop up during build.

Out-of-the-box access management is readily available. It gives you everything you need, so you can get to market when you need to.

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

Is IAM that much of a core competency of your business?

The answer is no.

Whether you're in Financial Services, Healthcare, Media or Consumer IoT, make sure your best developers are working on what makes your business boom.

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

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

Access management platforms let you externalise your authorisation, allowing you to change your business rules without changing your applications. This enables new security policies to be easily deployed and enforced across all your applications.

If you users can try out your service free for 30 days, but you want to extend that to 60 days, just update the access policy in the access management tool without changing your actual applications.

Simple.

## **9. Innovation** – Will your own access management continue to unlock new opportunities for you 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 of the work.

Stay ahead of the curve.

**Access management providers help you  
discover new business opportunities.**

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

Do you know all the prerequisites that are part of those standards?

Are you confident you won't accidentally descope features that are part of the standards?

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're coming from a different platform.

On a build project you have other priorities outside of adhering to standards. Don't compromise on standard specifications and buy.

## Conclusion

Economic factors aside, it's quick and simple to see the enormous benefits buying access management tools have. So, when you're faced with the choice of whether to buy or to build, the answer is simple – buy.