5 Fast Facts for API Access Control

APIs have become the defacto method for connecting people with data.

This is great news for users: access is much smoother and often instantaneous. But for administrators controlling sensitive data, access control is a major headache. With this in mind, we've outlined five key API access control facts – along with a little help on how to address them.

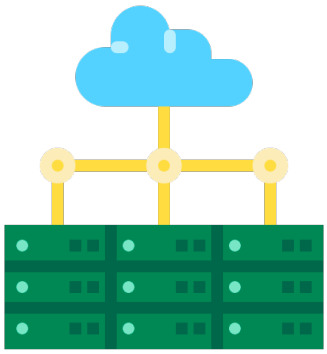
1. You Can't Predict the Future

When you develop an API it's designed to perform a specific task at the time of development. For this reason security is hard-coded into the system. But fast-forward six months; the user case changes and so do the user permissions – and the API authorization logic is no longer valid. Authorization changes need to be made, and quickly. And, if your business is like many others, your team is probably already hard at work on other APIs that need updating. If this sounds familiar, and you have to recode an API every time you need to make a change – externalizing authorization can help you solve this issue.

2. The Best Defense is a Good Offense

When companies carry out a risk assessment, most usually find that the risk of a data breach – due to unauthorized access – is high on the list of probabilities. But how do you mitigate this risk? You can't just sit back and wait for an attack to come: you need to be more offensive. You need to enable risk-aware access controls that go beyond perimeter protection and logging to protect business-critical data from being breached.

If you haven't ticked this problem off your list yet then risk-aware access control could be the best way to "defend" your sensitive data.



3. Context is King. And Queen... and Prince...

The in-built access controls in a conventional API Gateway are sufficient for many APIs. However, if you are dealing with sensitive data these controls will often fall short. By using context as a driver to determine who can access what data, when, how, for what purpose and from where – complex factors can be brought into the authorization equation. Data shared via an API becomes much more secure.

If you're not familiar with Attribute Based Access Control (ABAC), and would like to extend your API Gateway with context-aware authorization, we can help you.

4. You Can't Please All the People All of the Time

API Product Managers are often forced to prioritize business over security, or vice versa. When a new API is requested, business units will set key objectives. However, Security Managers will insist all policies and regulations are met and Auditors will expect you to be able to prove compliance – including who can access what information under what conditions. Despite this, launch date cannot be delayed.

If you struggle with this type of problem on a regular basis, then a policy-based access control approach to APIs could be the ideal solution for you.

5. Your Budget Will Only Stretch so Far

Change management is costly and time consuming. Once an API has been released there isn't much left in the budget. But when corporate polices change, these changes need implemented in APIs too. You have to juggle resources, and dedicate time that neither you nor your team have to spare. If only you could implement access control polices across all relevant APIs in one go – costs and resource requirements would be cut and implementation would be much quicker.

Centrally managing policies with an externalized authorization engine like the Axiomatics Policy Server enables you to implement policy changes across all your APIs in one go.

About Axiomatics

Axiomatics 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's Orchestrated Authorization strategy 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.

To learn more, please visit our website or follow us on **LinkedIn, Twitter,** and **YouTube.**

Learn more or request a demo of our solution:

axiomatics.com

webinfo@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240

AXIOMATICS