



SOLUTION BRIEF

Ultimate Access Control: Leverage Your APIs as Policy Enforcement Points

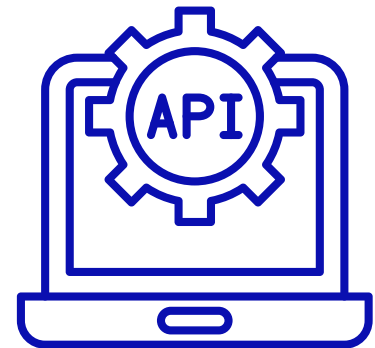
Axiomatics and Zuplo bring authorization to the API

API-first architecture provides organizations with a multitude of benefits such as scalability, reusability, flexibility for updates and generally speaking, faster time to market. However, an API-first approach requires the right level of security, routing, authentication, and authorization. This is where API gateways help organizations to reap the benefits of APIs while maintaining security and controls. In partnering with Zuplo, Axiomatics' externalized authorization capabilities to the API, enabling organizations to push access control policies out to their applications much easier.



Add attribute-based access control to API security

Zuplo enables organizations to protect their APIs by adding authentication, and rate-limiting in minutes as well as over 50 available plugins like caching with a single click. Zuplo provides a very easy way for security teams to insert the right level of protection for their APIs and provide peace of mind against threats like DoS and DDoS attacks. Now, partnering with Axiomatics, organizations can add [attribute-based access control \(ABAC\)](#) policies to their arsenal of protection and apply that to their APIs. ABAC evaluates multiple attributes from multiple information points in order to determine what actions can be taken, by who or what (be it an identity or another application), and under what context/conditions.



Leverage a policy-as-code approach

[Policy-as-code](#) removes security silos and combines configuration and compliance into one step. This enables organizations to employ testing and validation of the policies as part of a centralized process that also captures version control. Since developers are dealing with hundreds of applications, this approach also increases the speed and efficiency compared to a manual approach of addressing each API and application individually. The added benefit to this method is that any time a change in policy needs to be made, it can be done and pushed out through configuration as opposed to requiring code changes and downtime of the applications themselves.



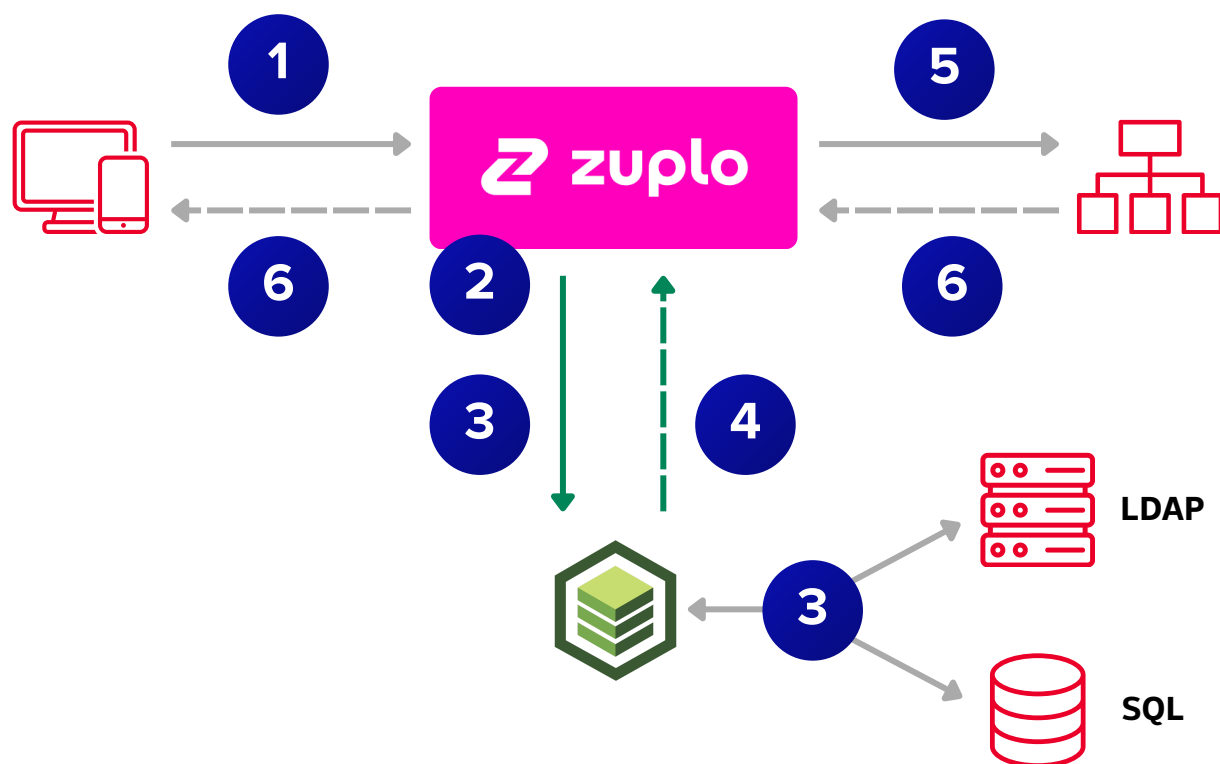
Follow the Zero Trust model

The goals of a [Zero Trust](#) model are to ensure continuous policy enforcement against critical attributes such as risk, time, location, classification, role, etc.. The Axiomatics-Zuplo partnership provides organizations with a central, dynamic, Axiomatics Zero Trust policy engine that removes the burden of coding and managing authorization functionality individually for each application. Instead, enforcement of these policy decisions are done through the Zuplo API gateway. This approach means organizations can employ a consistent set of compliance and security policies from one location and ensure they are applied across the organization's APIs, regardless of the underlying technology.



How does it work?

1. A subject (user or machine) calls out to the Zuplo API gateway.
2. The gateway determines which gateway policies (routing, rate limiting, transport, and authentication) apply and performs the authentication.
3. Once the user has been authenticated, Zuplo calls out to Axiomatics to determine whether the authenticated user is allowed to request the backend API.
4. Axiomatics returns a decision (Permit or Deny) along with additional metadata that may be used by Zuplo or the target API.
5. Zuplo's API Gateway forwards the decision to the application/resource.
6. The application/resource returns a response back to the subject.
 - a) Optionally, authorization can also be applied to the response payload by calling Axiomatics again for each part of the response.



For more information, or to request a demo, please contact us at info@axiomatics.com.

About Zuplo

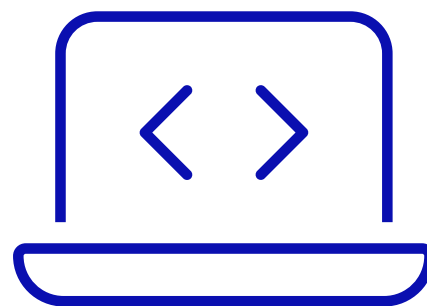
Zuplo is reinventing the API Gateway with a vision to democratize API Management, making it effortless to adopt and affordable to operate. We believe that shortening the feedback loop and helping teams move faster is the key to both building a better API and better outcomes for the business. We tackle this by embracing the modern developer workflow - rapid deployments (under 20s), gitops deployment, infrastructure as code, native support for open standards like OpenAPI, and being extremely programmable. Give it a try at portal.zuplo.com.



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