



SOLUTION OVERVIEW

Key Elements of a Policy-driven Authorization Solution

Whether it's a multinational enterprise or a small business, the sheer number of applications in use is staggering and organizations are trying to navigate a growing and increasingly complex tech ecosystem. In fact, on average, companies are using roughly 291 applications ¹. While this abundance of tools drives efficiency, it also presents a formidable challenge: managing access control across a sprawling and diverse environment.

But traditional access control approaches alone aren't enough. With so many applications and as many silos, users interacting in dynamic, distributed ways, enterprises need a more adaptable, secure, and scalable solution. This is where [policy-driven authorization](#) comes in.

Policy-driven authorization ensures users can only access what they are allowed to, based on a set of enterprise-wide and application-specific rules. These rules reflect the requirements compliance managers and application owners have defined. Rules use a wide range of attributes which might include the user's location, role, the time of day, the device being used, the resource in question, and the desired action they wish to perform. The purpose of this is to review all the attributes necessary to enforce secure authorization dynamically and in realtime ensuring security without compromising on usability or performance.

But what are the key elements of a policy-driven authorization solution? And why do enterprises need authorization?

Let's explore the key elements of such a policy-driven authorization solution and how it empowers organizations to navigate the complexities of access control while protecting data.

Why enterprises need policy-driven authorization

Enterprises today face significant challenges in managing access control across increasingly complex systems and applications. Traditional authorization models often operate in silos, with controls implemented inconsistently and without standardized frameworks. This fragmented approach makes it difficult to enforce authorization requirements or ensure secure operations.

Many enterprises also rely on hardcoding access controls within applications. By hardcoding authorization logic into applications, enterprises are opening themselves up to issues regarding scaling, compliance, and Shadow IT. As new users join and updates are added and need to be pushed to applications, making scalability become increasingly difficult. Compliance is an entirely new layer on top of this, adhering to regulations can cause more headaches for almost every business. Additionally, broad access controls can often lead to an "all or nothing" approach that frustrates users and drives them towards unauthorized tools and applications - known as Shadow IT. It introduces security risks, compliance violations, and a lack of visibility for IT teams, making it harder to protect sensitive data and enforce organizational authorization requirements. Policy-driven authorization overcomes these challenges by improving user experience, building applications faster, and enabling Zero Trust.

¹ https://chiefmartec.com/wp-content/uploads/2023/04/saas-count-and-spend_1456px.png

Improve user experience

A seamless and secure user experience is essential for maintaining productivity and collaboration in the modern workplace. However, when access controls are too rigid or obstructive, they can lead to frustration and unintended risks. In fact, one-third of employees admit to circumventing security measures that hinder collaboration, potentially putting their organizations at risk ².

Policy-driven authorization addresses this by enabling secure, adaptable, and frictionless access for both internal users and external stakeholders, such as suppliers and partners. By dynamically adjusting access based on real-time attributes — such as user role, location, citizenship, risk-score or device - organizations can ensure that collaboration is both safe and compliant without creating unnecessary roadblocks.

This approach to access control reduces friction, allowing users to work effectively in a way that adapts to their specific context. It fosters a secure environment where employees, customers, and partners can collaborate confidently, knowing that access is governed by precise, policy-driven rules.

Build applications faster

Many organizations are facing increased pressure to modernize their applications as part of broader digital transformation initiatives. However, as organizations embark on this journey, they often discover that traditional methods of implementing access control are inflexible and inefficient, limiting their ability to scale and adapt. This is where policy-driven authorization can help to make the applications scalable and flexible.

By partnering with an authorization vendor specializing in [attribute-based access control \(ABAC\)](#), enterprises gain access to proven tools and resources that streamline development. Vendors provide pre-built solutions that eliminate the need for internal teams to create authorization systems from scratch, saving time and avoiding budget overruns.

These solution providers 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. It also allows development teams to focus on delivering innovative features that are core to your business value proposition.

Policy-driven authorization externalizes access controls enabling centralized management of policies. This means changes can be made within the authorization engine and automatically applied across multiple applications - without the need to update application code itself. If you consider the average company has roughly 291 applications ³, this can become an enormous time savings instead of making these changes on every application.

Enable Zero Trust

For many organizations, traditional [role-based access control \(RBAC\)](#) has been a foundational approach to managing access for decades. However, as the complexity of environments grows, RBAC alone is no longer sufficient to protect sensitive and valuable information.

While RBAC assigns permissions based on predefined roles, it struggles to address the dynamic and context-sensitive nature of modern access needs. This often results in overprovisioning, role explosion, and conflicting policies across applications – leaving critical data exposed to unnecessary risk.

Legacy systems and networks, which were not designed with modern security principles like [Zero Trust](#) in mind, further complicate the picture. Many organizations rely on these systems to run key operations, making it essential to secure them without overhauling the entire infrastructure. Rather than replacing RBAC, ABAC complements and enhances it ensuring that access is granted only under the right conditions, providing the adaptability required to protect legacy systems.

By incorporating policy-driven authorization, ABAC ensures that access decisions are based on reliable, real-time data, giving organizations the confidence to verify every request with precision. It serves as an excellent starting point for a Zero Trust implementation, safeguarding critical assets by ensuring they are accessed only by the right people, in the right way, at the right time.

This alignment with the core methodology of Zero Trust makes policy-driven authorization a crucial solution for modern enterprises seeking to strengthen their security posture.

Elements of policy-driven authorization solution

The benefits of policy-driven authorization are interconnected, providing enterprises with the specific controls and flexibility needed to achieve their goals. To maximize these advantages, organizations must focus on key elements within an authorization solution that address their unique challenges.

Elements of an authorization solution



Flexibility



Centralized reporting



Performance



Extensive
attribute connectors



Centralized policy

Flexibility

When it comes to creating access control policies, administrators have the full power of the policy language at their disposal. What matters most is that the policies align with the organization's core business outcomes. Some teams prefer a developer-focused approach to crafting policies, relying on technical precision and coding, while others lean toward a user interface (UI)-focused method, emphasizing ease of use and accessibility for non-technical stakeholders.

An adaptable policy creation process helps accelerate application development. By enabling developers and non-technical users to collaborate seamlessly, organizations can reduce miscommunications, streamline workflows, and avoid bottlenecks. When the process accommodates both technical and business perspectives, teams can quickly draft, review, and refine policies, leading to faster deployments and updates.

At Axiomatics, [our solution](#) is designed to support multiple user profiles in ways even non-experts can understand. Business users can draft policies in standard English, which can then be converted into the underlying policy language, [ALFA](#), for developers to evaluate. Similarly, policy authors can present policy implementations in ALFA and instantly convert them into plain English for business users or auditors to review. This bidirectional capability not only enhances collaboration, but also ensures that policies are transparent and easily auditable, making compliance processes smoother and more efficient.

The ability to craft policies in various formats and seamlessly translate between them ensures that the right method is applied to the right scenario, reducing friction and enabling teams to build secure, scalable applications more quickly. This flexibility is a hallmark of modern policy-driven authorization solution, empowering organizations to align security with business goals while maintaining agility.

Connection to data sources

Many organizations are in situations where user-information data is often distributed across multiple systems, such as an active directory, databases, Workday, and security tools like CrowdStrike. Effective policy-driven authorization requires the ability to pull relevant attribute data from any of these sources in real time to make precise access control decisions. Without this capability, organizations risk enforcing outdated or incomplete policies that do not reflect the latest user context.

Data connectors solve this challenge by enabling seamless integration with various data sources, ensuring that access decisions are always informed by the most up-to-date attributes. This approach allows organizations to enforce fine-grained, context-aware access control that adapts dynamically based on factors such as user role, device type, location, and security posture. By leveraging real-time attribute retrieval, enterprises can maintain both security and operational efficiency without compromising user experience.

This dynamic approach to access control aligns directly with Zero Trust principles, where no user is inherently trusted and all access requests must be continuously verified. ABAC ensures that every access decision is evaluated based on current attributes, eliminating static and overly permissive access models. With an authorization solution that supports a wide range of data connectors, enterprises can confidently implement a Zero Trust framework, ensuring that access is continuously verified and granted only to the right users under the appropriate conditions.

Performance

In any security initiative, performance is a critical factor that directly impacts user experience and overall system efficiency. A responsive and fast authorization solution ensures that users – whether they are customers, employees, or partners – can interact with systems seamlessly while maintaining security and compliance. When policies enable nuanced decisions including conditional access, businesses can continue operating smoothly, sales can progress, and sensitive information remains protected.

To achieve this balance, policy-driven authorization incorporates two key elements: attribute data caching and robust Policy Decision Points (PDPs).

Attribute caching enhances performance by temporarily storing frequently used data for a customizable period. Without caching, the system would need to repeatedly query the source for attributes, introducing unnecessary delays. With caching in place, access decisions can be made faster, ensuring that users experience minimal friction while sensitive data remains secure.

That being said, attributes can be cached, but only if it is acceptable from an authorization perspective to use that stale attribute value. It is important to note that this is not done with dynamic attributes, like time of day or exchange rates, which can change frequently. It is only done with more static attributes such as roles, which don't change as often. Additionally, there are also settings around how long each attribute value can be cached.

Organizations need a PDP that can handle high traffic loads without crashing or slowing down. A reliable and scalable PDP ensures that even during peak demand – or under the stress of a distributed denial-of-service (DDoS) attack – the system can continue making rapid and accurate access decisions. For instance, a customer shared that during a DDoS attack, their PDP was the only component still standing, providing them with a critical layer of resilience and confidence in their security architecture.

Performance is not just about speed; it's a fundamental enabler of modern security strategies like Zero Trust. In a Zero Trust framework, where “never trust, always verify” is the guiding principle, every access request must be evaluated dynamically based on real-time context. Slow or unreliable authorization processes can undermine this approach, creating bottlenecks and frustrating users.

By combining attribute caching with high-performance PDPs, policy-driven authorization supports the rapid, context-aware decision-making required for Zero Trust while also delivering a superior user experience.

Centralized reporting

Traditional RBAC approaches often suffer from fragmented reporting, where access information is siloed across various applications. This makes it difficult, if not impossible, to maintain a comprehensive view of who has access to what resources. When audits are conducted, they frequently rely only on the limited data available within individual systems leaving significant blind spots. In many cases, organizations must manually compile logs from disparate applications to generate access reports. This process is time-consuming, inefficient, and prone to errors.

Policy-driven authorization eliminates these challenges by providing centralized reporting that consolidates access data across all systems. With the help of ABAC, authorization decisions are made dynamically using multiple attributes and the authorization engine generates detailed audit logs for every access request.

These logs create a complete trail of access activity, recording who accessed what data under what conditions, and whether the request was granted or denied. Such centralized reporting not only simplifies audits, but also provides valuable insights into usage patterns. This enables organizations to optimize their access policies and ensure compliance with security regulations.

A unique advantage of policy-driven authorization is its ability to facilitate comprehensive access reviews and “what-if” scenarios. By leveraging the rich data captured in audit logs, enterprises can simulate potential policy changes, assess their impact, and ensure that the right people have the correct level of access to sensitive information.

Centralized reporting also plays a critical role in enabling Zero Trust security. The Zero Trust model emphasizes continuous verification, requiring real-time visibility into who is accessing resources and why. By providing a single source of truth for access activity, it strengthens compliance, enhances security, and supports the Zero Trust framework, ensuring that access to critical resources is always transparent and under control.

Centralized policy

In large enterprises with multiple applications, authorization is often managed in silos, leading to inconsistencies and security risks. However, a policy-driven authorization solution addresses this challenge by centralizing policies that can be written and deployed uniformly across the entire application and data ecosystem. This approach ensures that access is controlled consistently and efficiently, eliminating the risk of excessive permissions caused by fragmented, application-specific policies.

For example, a manufacturing company with hundreds of homegrown applications or microservices all with their own policy sets might struggle with inconsistent access across systems. Depending on which application is used, some users may inadvertently receive excessive permissions simply because the application does not support granular controls, threatening the security of the application. Policy-driven authorization solves this by applying centralized, dynamic policies that are enforced consistently across all applications.

When authorization is hard-coded into individual applications as an afterthought, developers often adopt a “minimum viable solution” approach. This type of approach focuses on getting the software operational while leaving complex authorization challenges unresolved. Over time, this creates technical debt that can lead to costly rework and security vulnerabilities.

By contrast, with an externalized authorization solution, policies can be centrally managed, written once, and applied across multiple applications. This reduces development time by approximately 20%, as developers no longer need to code and maintain authorization logic within each application. Future updates can be implemented seamlessly with no need to redeploy or interrupt application uptime.

Additionally, a centralized solution ensures that compliance and security policies are consistently applied across the organization, regardless of the coding languages or platforms in use. This consistency not only strengthens the organization's security posture, but also simplifies compliance processes which provides auditors with a single source of truth for policy enforcement.

Conclusion

Policy-driven authorization offers a dynamic solution that enhances security without compromising usability. By leveraging real-time attribute evaluation, organizations can ensure the right users have the right access – at the right time, under the right conditions.

This approach offers key benefits: it enhances security by enabling Zero Trust, ensuring access is granted dynamically based on real-time context. It improves user experience by providing seamless, contextual access without unnecessary roadblocks. Additionally, by externalizing authorization, organizations can accelerate application development, eliminating hardcoded policies and simplifying policy management.

To fully realize these advantages, a robust policy-driven authorization solution should include:

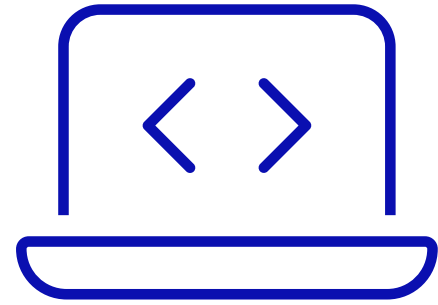
- **Flexibility** to support both developer-driven and business-friendly policy creation.
- **Extensive attribute connectors** that integrate with multiple data sources for real-time access decisions.
- **High performance** to enable fast, scalable decision-making without latency issues.
- **Centralized policy & reporting** to enforce consistency and simplify compliance audits.
- **Advice & obligation** features that provide guidance and enforce security conditions dynamically.

By implementing policy-driven authorization, enterprises can confidently navigate the complexities of access control, securing sensitive data while driving business agility and compliance.

Take the next steps

Learn how 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