AXIOMATICS

WHITEPAPER

Why traditional IAM solutions are no longer enough

How attribute-based access control augments your protection

Table of Contents

01 Background

02 Why is IAM no longer sufficient?

03 Attribute-based access control

04 NIST approach to ABAC

05 Implementing ABAC

06 Next steps

Background

IT organizations have always confronted a diverse set of challenges. They are often faced with hundreds or even thousands of disparate applications each running in their own stove-piped deployments. These applications run the gamut of brand new, to legacy or even unsupported software. IT departments are also up against an array of regulatory and security compliance requirements, while navigating a post-Covid world where many employees now work remotely.

To address these challenges, organizations traditionally leveraged IAM solutions to ensure their workers get the access they need to the data they need to do their jobs. Over the last decade, thanks in part to multiple compliance mandates and high-profile breaches, organizations shifted focus to ensure workers get only the access they need to only the data they need, and nothing more.

This creates a balancing act, ensuring IT departments aren't slowing down the business' ability to do what it is they need to do to be successful, while also ensuring the security and governance of the data they are entrusted with.

The challenge Chief Information Security Officers (CISOs) now struggle with is whether they apply too much security resulting in no one being able to do their jobs in a timely fashion or apply too little security so their organization ends up as a news story due to a costly public breach. It can be viewed as a no-win situation and perhaps the reason why the average tenure of a CISO is just 26 months.

Why is IAM not sufficient ?

Identity and Access Management (IAM) solutions are an amazing advancement and have saved countless headaches and work hours for today's IT professionals.

Without these solutions, organizations would need to manage each application's and user's access separately. It would be a world of spreadsheet tracking without consistency between organizations.

With an IAM solution, all of this can be identified, users can be authenticated, policies can be established, and access can be monitored and reported.

So why is IAM no longer enough? The problem is a continuous stream of changes. People leave and start new roles either within the organization or elsewhere, new compliance regulations are introduced, new applications and hardware are added, and so on.

Role Based Access Control (RBAC) was introduced and addressed some of this. IT would assign a user to a role and policies would be established to clearly state what a specific role could or could access or do. This was often tied to and synched with the HR system. When a new user would be hired, based on their job title the IAM solution would assign them to a role.

If their job title changed due to a transfer or if they left the organization altogether, the IAM system would capture this once it synched with the HR system and the change would be made. Sounds simple enough, and it helped, but in a world of constant change, most IAM solutions don't account for the context of other changes.

Context is key because without it, the IAM solution misses key elements necessary to make an appropriate decision about whether to grant or deny an access request. According to the 2021 Verizon Data Breach Investigations Report, social engineering is now the number one pattern in breaches and credentials remain an attacker's top target. If a bad actor tricks an employee into somehow exposing their credentials, authentication and RBAC policy review alone won't necessarily identify any risk of exposure. The scenario below illustrates this.

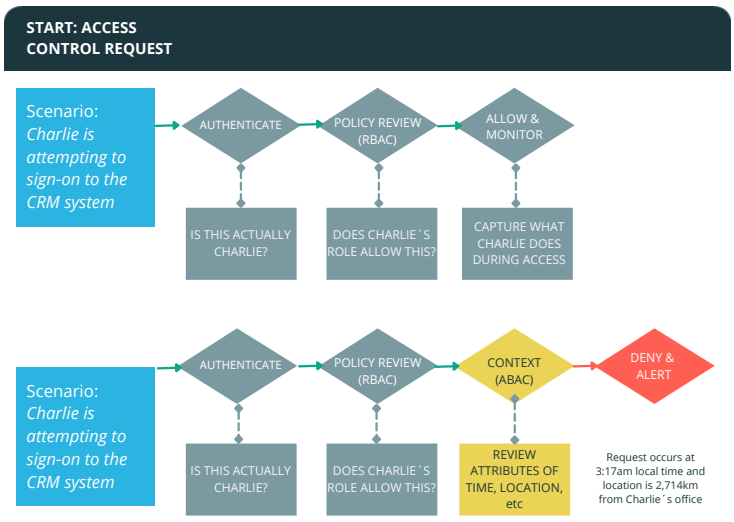


Fig. 1: The above example shows how the same scenario results in a different outcome when context is reviewed.

Attribute-based access control (ABAC)

Attribute-Based Access Control (ABAC) is typically used to safeguard data in applications, databases, microservices and APIs, within complex architecture.

Instead of just looking at the role, ABAC is used to grant access based on other attributes such as a user's location, the time of day, the device being used, the resource in question, and the desired action. The purpose of doing it this way is to review all the attributes necessary to enforce secure authorization dynamically and in real-time.

Put simply, attributes act like the levers in a lock, in that all of them must be aligned – with a policy – before access to data is granted. In the scenario above, Charlie still held the same role and under policy, that role is permitted to access the CRM system.

However, it's the attributes of time and geolocation that were deemed out of policy and resulted in a denial of access, with an alert sent to notify and take appropriate action.

The NIST approach to ABAC

As the ABAC method further eliminates risks from inappropriate access, it's not surprising the National Institute of Standards and Technology (NIST) recommended adoption.

The National Cybersecurity Center for Excellence (NCCoE) a part of NIST, summarizes in the NIST Special Publication 1800-3A: Attribute Based Access Control, that:

"Its dynamic capabilities offer greater efficiency, flexibility, scalability, and security than traditional access control methods, without burdening administrators or users."

NIST first recommended ABAC adoption back in 2014 with the release of SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations. However, in response to slow adoption, the NCCoE developed an example of an advanced access control system to provide organizations with what they refer to as a "How To" guide in SP 1800-3. Sections of this special publication describe the approach and architecture followed by detailed walk through guides on configuration and set-up.

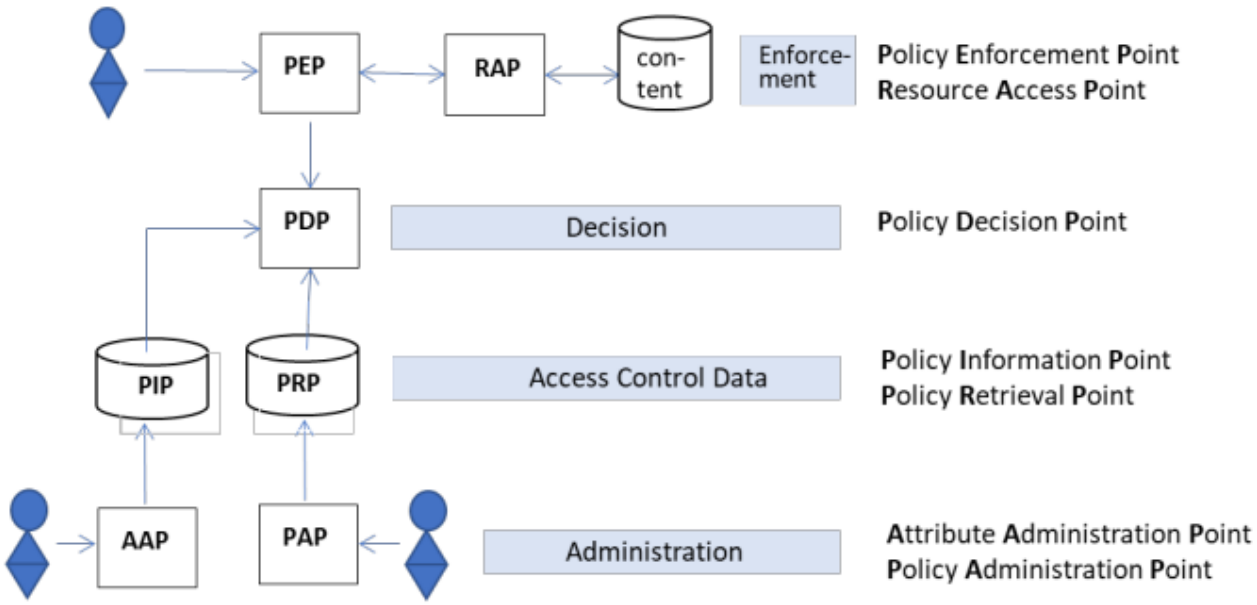


Figure 3.1 ABAC Functional Architecture based on XACML Representation

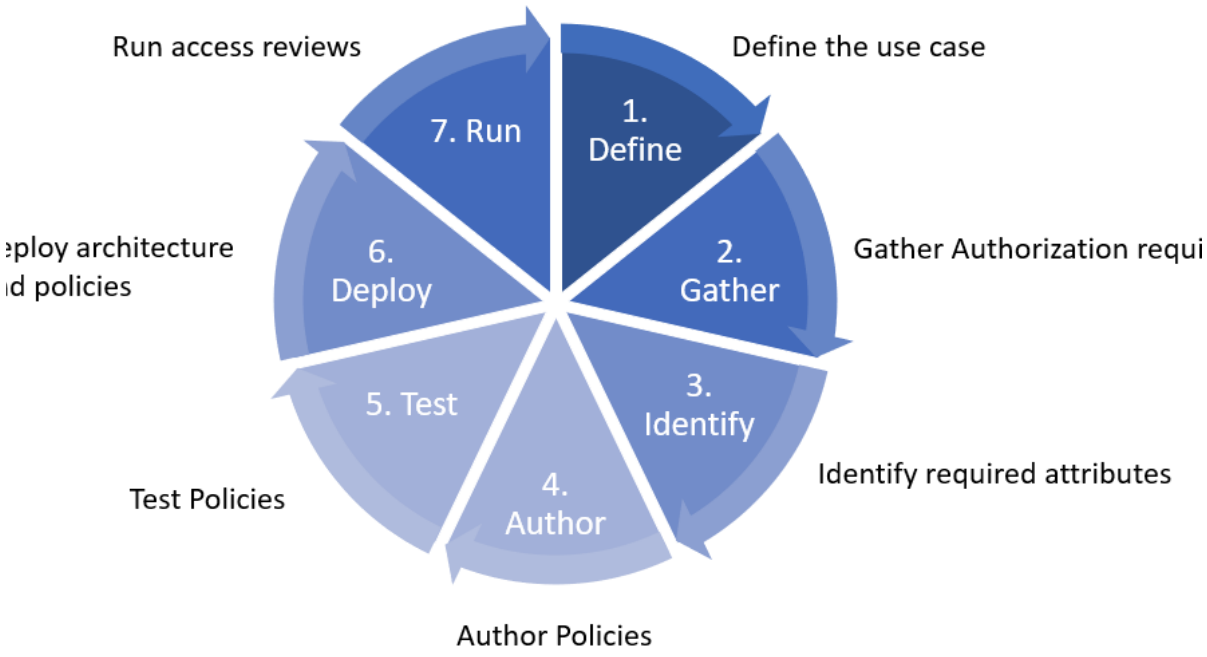
Implementing ABAC

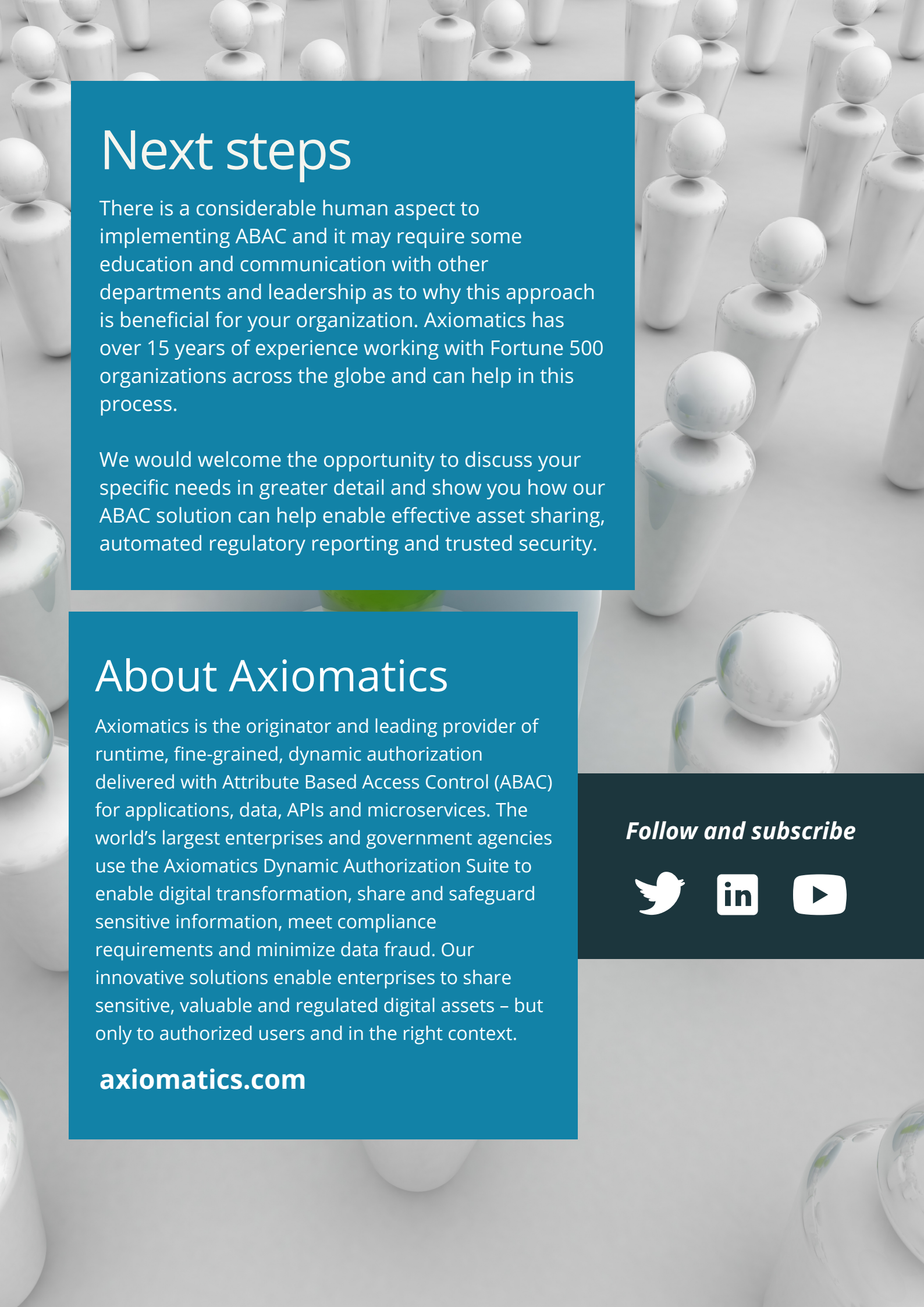
The successful implementation of ABAC in an enterprise IAM environment requires careful consideration of enterprise attributes and digital policies. This is not an exercise you take with speed as the main goal. You will want to take the time to get things right, because after all, this is being undertaken to protect access to your organization's (and your customers') data. Before your organization tackles this challenge, you also must understand that unlike traditional approaches such as RBAC, in ABAC a user's entitlements are not directly assigned to the user via roles and permissions.

Instead, a user's entitlements are the result of a runtime authorization request evaluated against a set of policies. This is a different way to approach access and means access reviews in the traditional sense are no longer effective. Traditional provisioning and deprovisioning are no longer sufficient. ABAC will require new processes and new authorization requirements will need to be gathered. So, where do you begin? Axiomatics has been assisting customers with this process since 2006 and have found that the following approach enables organizations to successfully move to an ABAC model.

7 STEPS APPROACH

Authorization policy life-cycle





Next steps

There is a considerable human aspect to implementing ABAC and it may require some education and communication with other departments and leadership as to why this approach is beneficial for your organization. Axiomatics has over 15 years of experience working with Fortune 500 organizations across the globe and can help in this process.

We would welcome the opportunity to discuss your specific needs in greater detail and show you how our ABAC solution can help enable effective asset sharing, automated regulatory reporting and trusted security.

About Axiomatics

Axiomatics is the originator and leading provider of runtime, fine-grained, dynamic authorization delivered with Attribute Based Access Control (ABAC) for applications, data, APIs and microservices. The world's largest enterprises and government agencies use the Axiomatics Dynamic Authorization Suite to enable digital transformation, share and safeguard sensitive information, meet compliance requirements and minimize data fraud. Our innovative solutions enable enterprises to share sensitive, valuable and regulated digital assets – but only to authorized users and in the right context.

axiomatics.com

Follow and subscribe