NEXTLABS®

White Paper

How to Ensure a Successful ABAC Implementation

The NextLabs Solution Architecture

Attribute-based access control ("ABAC" for short) has reached the point of mass adoption with respect to access control technologies. In fact, the National Cybersecurity Center of Excellence developed a reference design for ABAC that provides organizations "greater efficiency, flexibility, scalability security." To ensure that those benefits are realized, however, it's essential to establish best practice guidelines when it comes to implementing ABAC successfully.

ABAC can be instrumental in reducing enterprise risks such as insider threats, loss of customer data and personally identifiable information (PII), leakage of trade secrets and intellectual property, and fraud. The use of context in access decisions can also lead to substantial cost savings since ABAC systems enable more efficient policy management and regulatory compliance. Furthermore, organizations can continue to leverage much, if not all, of their previous investment in existing IT infrastructure.

1. Attributes - It Is All About Quality, Not Quantity

A major advantage of using attributes, rather than roles, as the focal point for access control is that it emphasizes quality over quantity. It is not the sheer number of attributes that matters – it is the ones that are selected. You can have all the attributes in the world in your policies, but it will not amount to much if the right ones are not selected. What makes ABAC so powerful is that it adds a dynamic element to access control, which enables organizations to make accurate, real-time business decisions based on the latest information.

For instance, in the past, with an RBAC-only approach, you might need 1,000 roles to account for every possible scenario with respect to a group of employees' roles and permissions within a department. However, with an ABAC approach, you can simplify this to just one policy to achieve the same results. Additionally, you wouldn't have to spend countless IT hours updating roles and permissions every time someone changes jobs or gets assigned to a new project.

Here's an example illustrating the power of ABAC and how one policy can replace thousands of roles with just two or three attributes: Acme Company has 15 locations globally, 12 functional areas ("departments"), and 20 ongoing projects per department. Doing the math, that's 3,600 roles (15*12*20), which essentially can be replaced with one ABAC policy using three data attributes (location, department, and project).

2. Apply Access Control Policies By Core Business Processes And Common Data Sets

Applying a consistent set of policies across key business processes will reduce complexity and cost. This is accomplished by adopting a global approach to access control – one in which you design and develop a common set of reusable policy components and policies to enable global access for each set of business-critical data (e.g., intellectual property, trade secrets, financial data, PII, controlled technical data, etc.).

For example, if you could have one set of GDPR policies that works across multiple applications, this obviates the need to have a separate set of GDPR policies for each application where PII data resides. This leads to less administrative burden, lower application development costs, and more agility to respond to dynamic market and regulatory conditions.

Another example is export controls. Typically, export control regulations impact data stored in various sources, including ERP, CRM, PLM, and SharePoint, among others. Knowing that controlled technical data (CTD) can be found in so many different applications, what and how CTD is managed by those applications sets the stage for creating the most appropriate and effective set of policies to enforce across all relevant applications.

3. Master Data Drives Attributes - Quality Of The Mater Data Is Essential

In today's businesses, data is a valuable corporate asset which, when managed properly, can support a company's ability to achieve its strategic goals and financial results. A recent Hackett Group study revealed that over 70% of companies are planning to implement a business intelligence system, establish data stewardship rules, standardize master data, and cleanse existing data – all of which are elements of a sound Master Data Management (MDM) strategy.

Master data is the core data that is essential to operations in a specific business or core business process. With good master data, you can effectively implement ABAC policies to meet your business requirements. The data can pertain to customers, materials, vendors, suppliers, and much more. Master data in ERP systems is the foundation upon which business transactions are executed. Incorrect or incomplete master data will have a direct impact on key business operations. Most companies manage master data in multiple MDM systems. These MDM systems store master data centrally and serve as a single source of master data to ensure consistency across all key business applications.

Since most companies have already defined and managed a rich set of useful master data and metadata in their MDM and business applications, this master data forms the foundation for a reliable source of attributes used to derive ABAC policies and is critical to implementing ABAC successfully. Common examples of trustworthy sources of metadata are MDM, IAM, and several critical business applications such as ERP and CRM.

4. Dynamic Trumps Static: A Small Number Of Real-Time Policies Will Get The Job Done

In the same vein as #1 above, policy management need not be complicated. Unlike traditional access control techniques, you don't need many policies to meet your access control requirements. When implemented correctly, a handful of policies can get the job done across all business-critical applications. The key is deciding on the criteria (i.e., conditions) to control access and apply the same criteria consistently across the entire organization. In other words, policies should be designed to use a common set of criteria to work across applications.

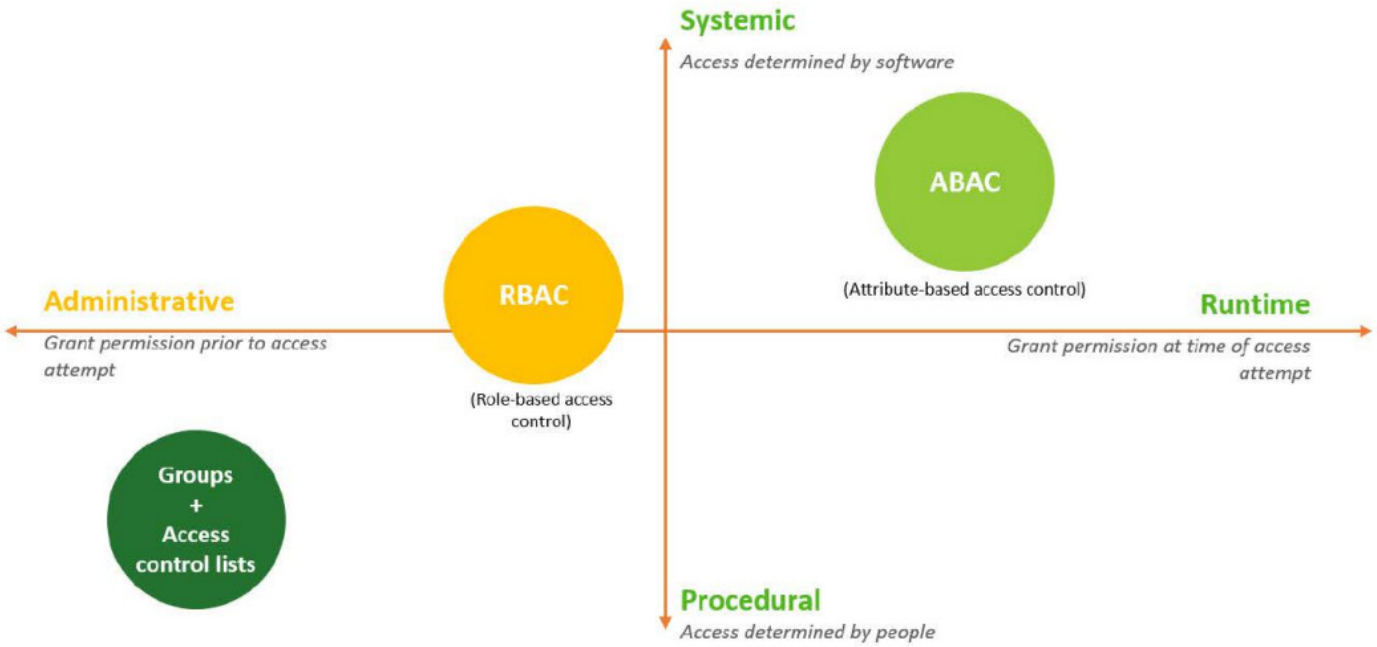
Because ABAC policies are evaluated in real-time, there is no longer a need to deal with ongoing change management. ABAC enables enterprises to apply a consistent set of policies across business-critical applications to address complex internal controls, security, governance, risk, and compliance requirements, saving organizations much time and money.

5. ABAC Is Not Only For Structured Data - It Is For Unstructured Too

Nowadays, more than 75% of business-critical unstructured data (i.e., documents and files) originates from data managed by applications. But, with so many documents and files being shared internally and externally, an approach that applies a consistent set of policies to protect data whether it sits inside or outside of an application are most favored by IT and security practitioners. And that's where ABAC shines. It's the underlying technology that enables data, whether it sits inside or outside the application, to remain safe. ABAC can be applied to both structured and unstructured data, which is important, given the need to share information so that businesses can collaborate with partners and customers, build new products, collaborate on R&D projects freely, or simply put, just get work done.

6. RBAC And ABAC Can Co-exist

Contrary to popular belief, ABAC can complement, but does not always need to replace, RBAC. RBAC may indeed be an older technology, but it still has a place in today's IT environments for many customer requirements. As a result, ABAC actually increases your ROI on RBAC since you can leverage the RBAC policies you've already created and make them applicable to today's more complex IT landscape (e.g., cloud, on-premises, mobile, IoT, telecommuting, etc.). In other words, you can overlay ABAC on top of RBAC, enabling you to derive more value out of your existing applications. Finally, you also avoid migration headaches as you'll still be leveraging the RBAC model.



ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.