AXIOMATICS

Business Case

Making a Business Case for Attribute Based Access Control (ABAC):

Cut Costs, Streamline Access Control and Achieve Compliance

Overview:

You are spending too much time and money managing access control and it’s not meeting your security expectations.

Many security architecture teams across the Fortune 1000 estimate that some 20-40% of security architects’ and developers’ labor hours are spent managing access control. Multiply that by an ever-increasing portfolio of applications, databases, APIs, user permissions, and the average Fortune 1000 company is looking at spending far too much of their annual budget on security costs.

Additionally, the relative cost to fix code issues throughout the application maintenance lifecycle also impacts user productivity. As noted by The National Institute of Standards and Technology (NIST), code fixes on systems in production come in at an estimated 30 times the cost of fixes performed during the design phase.

How much are you spending on access control?
Use this formula for a quick calculation.

624 X #SA/D X $AHR = $

- 624 – 30% of 2080 (total labor hours/year)
- #SA/D – number of security architects/developers
- $AHR – average hourly rate in dollars
- $ – dollars spent annually on security costs

To top it all off, today’s authorization measures are fraught with security risks. Antiquated access control systems allow authorized users access to sensitive data that should not be accessed within their particular job function or level of security clearance. Leaks, fraud, identity theft, and other compliance issues are commonplace in systems that weren’t designed for today’s distributed and complex environments.

And if your enterprise wants to expand into new areas (perhaps by creating external or customer facing portals or applications), the logistical challenge only increases–as does the risk a company faces when exposing sensitive data to new user populations.

How mature is your access control?

- Do you have access control rules scattered across the application code?
- Do you have access control rules implemented as part of the application business logic?
- Do you resort to maintaining application code in order to update your access control policies?
- Do you struggle to implement policies such as segregation of duty?
- Do you need to take into account context, such as location, time of day, or device type with regard to your access control policies?
- Are you concerned about the increasing number of roles in your access control matrix?

Axiomatics saves enterprises time and money while minimizing risk and maximizing functionality.

There are several core problems responsible for the rising time, cost, and risk associated with managing access control across an organization:

1) Lack of centralized authorization management
2) The increasing complexity of business environments
3) The cost and complexity of reaching and maintaining compliance with regulatory standards

Axiomatics addresses these problems head on. By externalizing authorization out of the infinite application and data silos in which they currently reside, Axiomatics reduces the amount of time spent on access control maintenance annually. And by implementing policies using context-aware Attribute Based Access Control to augment Role Based Access Control approaches (RBAC), Axiomatics reduces risk while increasing functionality exponentially.

> “Instead of making authorization decisions about a user based solely on his/her role, ABAC allows an enterprise to make decisions about access based on any number of attributes that can be defined by access control policies in real-time.

Problem #1: Lack of centralized authorization management increases the time and money spent managing authorization.

Existing authorization systems often involve hardcoding user and data access information locally, meaning that each and every application and database has its own version of a user’s access information. This was manageable when applications were few and the amount of data limited, but today's sophisticated environments have greatly increased the time and money spent managing each user and his or her access across multiple domains and applications.

When access rules change in the future – which they likely will, many times over – a programmer will be required to manually change the rules that have been hard coded into the application or database. This process requires considerable time and effort on behalf of the development staff, and limits the enterprise's ability to react quickly to changing requirements.

Problem Solved: Manage your authorization centrally (not locally) to save time and money.

Just as user administration and authentication are now largely managed centrally thanks to virtual directory environments or federated identity systems, Axiomatics manages authorization in a centralized service using an Attribute Based Access Control approach.

No matter how many users, and no matter how many applications or databases an enterprise might have (or may have in the future), access controls no longer have to be hardcoded into programs individually. Instead they can be externalized from those silos and defined, managed and rolled out from the centralized authorization service, cutting time and money spent on authorization exponentially.

Problem #2: The increasing complexity of business environments maximizes risk and limits functionality.

Despite a growing user population and ever more sophisticated business requirements, most companies still rely exclusively on legacy authorization systems that use Role Based Access Control (RBAC).

RBAC was originally designed to answer the question: What access does a user have based on their assigned role(s)? That role would then act as a golden ticket, allowing a user access to various information and/or actions based on permissions associated with that role within each requested application or database.

But expanding user populations (partners, consumers, regulators, auditors, etc.), and multi-role users, not to mention rapidly escalating application and database complexity, require fine-grained authorization. Authorization that not only answers the question "What is a user's role(s)?" But also: "Who is that user related to?" "What resources should he/she have access to?" "Where is data being accessed from?" and "At what time?"

Without understanding the context around a user, authorization is limited to making decisions based solely on his or her role(s) within an organization. But roles are not one-size-fits-all, and two users with the same role might require different authorization access (in fact, more than likely they do). Assuming otherwise can be dangerous, giving users access they shouldn't have, and putting your organization at risk for fraud, theft of sensitive data, and compliance issues – including the separation of duty or toxic combination challenges.

Additionally, all of these changes need to be entered manually, dramatically increasing the capacity for human error and upping the ante on risk. If a user's information is accidentally updated in one directory but not another, a user may have conflicting stories being told about his/her role within an organization–stories that could unintentionally allow him/her access to information he/she should not be able to access.

> “Axiomatics authorization services provide externalized authorization systems using ABAC for finer-grained authorization, saving your enterprise time and money.

Problem Solved: Build upon an RBAC foundation with ABAC for increased security and maximum functionality.

In 2013 Gartner predicted that, "by 2020, 70% of all businesses will use Attribute Based Access Control (ABAC) as the dominant mechanism to protect critical assets, up from less than 5% today." This trend has been spotted across vertical markets and government agencies as teams are rapidly adopting ABAC.

Instead of making authorization decisions about a user based solely on his/her role, ABAC allows an enterprise to make decisions about access based on any number of attributes that can be defined by access control policies in real-time.

Users can be permitted or denied access based on attributes such as who they work with or what projects they have access to, where the individual is based or where their device is currently located, what time of day they attempt access, and why they might need it. In other words, complex policies can be defined allowing access based on any number of attributes, not just roles.

And the good news – you're already part of the way there if your existing access control is based on users' roles, as roles are one aspect of an attribute-based approach. You'll be able to take your current investment and begin making the shift to contextually-aware access to your applications, databases, or third-party integrations. With ABAC you can protect sensitive data and Intellectual Property and meet compliance – all while better serving internal and external customers.

Problem #3: The cost and complexity of reaching and maintaining compliance with regulatory standards

The global economy is enforcing privacy laws and regulations both regionally and nationally. In the financial sector, privacy laws are being enforced by jurisdiction throughout the EU, while Singapore's Personal Data Protection Act of 2012 is typical of stricter country-specific regulations.

Furthermore, across industries where Personally Identifiable Information (PII) is regulated, such as health care and insurance, regulatory guidelines are being rigorously enforced – with massive fines in the case of non-compliance. Regardless of what industry you operate in, the number of regulations are increasing, and compliance is putting greater demands on how you manage data access.

For example, some regulations surrounding PII are now specific with regard to the requirement that privacy must be protected by means of encryption – and very specific about under what circumstances personal data relating to a specific citizen may be processed, transferred or stored. These regulations require enterprises to implement complex security measures that couple security techniques such as encryption, with a fine-grained approach to authorization – ensuring a context-aware approach to access control.

Problem Solved: Achieve and maintain compliance with ABAC.

ABAC provides the ability to make access control subject to business policies that can be edited to adapt to new circumstances and changes – dynamically and specifically to meet the growing number of regulations.

The framework of ABAC is application and database security controlled by fine-grained authorization rules. This determines who gets access to what based on the purpose of use, the context, and all the other dynamic conditions that are typical for privacy-related use cases.

A benefit in migrating to ABAC with Axiomatics is the ability to enforce these policies on multiple levels in your infrastructure -applications, APIs, and databases –and on a regional or countrywide basis, through a centralized services manager.

Use Cases in Action

How Axiomatics saves you time and money. And gives you fine-grained access control for heightened security and increased functionality.

Axiomatics authorization services provide externalized authorization systems using ABAC for finer-grained authorization, saving your enterprise time and money, while mitigating risk and increasing functionality. But Axiomatics goes well beyond merely "solving the problem" common to security approaches today.

Here are several ways we work with customers in the financial, government, manufacturing, and health care industries to not only solve current authorization issues, but to go beyond them, enabling future-proof authorization.

The Use Cases

How Axiomatics works for different industry verticals.

In the Financial Sector:

A large global bank operates offices in different countries on several continents. They employ hundreds of bankers who manage many thousands of clients. But each country has its own business rules and privacy regulations about who can access what data. And each banker requires access to information about only those clients to which they are assigned. Without a fine-grained authorization system in place, bankers could have access to sensitive information that they are not entitled to, thus making the bank non-compliant.

By rolling out ABAC, Axiomatics Authorization Services enable the global bank to specify which banking locations have access to which records, as well as which bankers have access to which client's information. In this way, the bank can decide that branches can only have access to records of customers in their own region or country, and only bankers assigned to specific clients, can have access to those clients' records.

In the Government Sector:

A large federal government agency oversees several law enforcement agencies that each operate within a given jurisdiction. A state law enforcement agency needs access to specific information about a case that occurred within a local law enforcement jurisdiction. And the federal government agency needs overarching case data relevant to both law enforcement agencies. But each agency requires different information from the case and for a different purpose; access to too many details on the part of any agency could result in a critical data breach.

Axiomatics Authorization Services enable fine-grained access control that can delineate which agency has access to what case data, when, for how long, and for what given purpose. Because of these policies, the state agency gets access only to the case data relevant to its specific purposes, and the overseeing federal government agency has access only to information pertinent to its authoritative means.

In Manufacturing:

Manufacturing Brand Z owns several brands that each manufacture their own set of products. In order to protect intellectual property, it is imperative that Brand A has access only to manufacturing details pertinent to Brand A, and that Brand B has access only to manufacturing details pertinent to Brand B. Not to mention, Brand A manufactures several lines of products and needs to be sure that employees working on Product C don't have access to sensitive data about Product D.

Axiomatics Authorization Services keep intellectual property secure by allowing Brand A access to manufacturing data relevant only to Brand A, and Brand A's employees access to manufacturing data relevant only to the specific product on which they are assigned to work. Thereby keeping sensitive product data secure while enabling access to those that need it.

In Health Care:

A large health care organization operates several hospitals that each employ hundreds of employees and serve thousands of patients. Each hospital works with a variety of constituents including insurance companies and pharmaceutical companies, as well as outsources patient needs to specialists and laboratories. Each party needs access to different information about a patient and his or her health, something that is not easily achieved with legacy data systems.

Axiomatics Authorization Services are deployed to offer fine-grained authorization that gathers attributes about a patient and enforces policies dependent on them. A patient can now have direct access to his or her health records, as will doctors assigned to that patient, while insurance companies may have access to the diagnosis, and labs may have access to blood samples but not the reasons for ordering them.

By implementing ABAC with Axiomatics, appropriate parties can see all of the information they need, and none of the information they don't. This ensures a efficient and faster service, while complying with data privacy regulations.

If the database load is intense, performance may also depend on how the Axiomatics Data Access Filter is deployed. The architecture is modular to allow for different deployment scenarios as to not affect performance.The product can be deployed for load balancing in different ways. Multiple instances of SQL Proxy Servers (each with different SQL Proxy Services running) can be deployed behind a load balancer.

Multiple SQL Filter Services can also be deployed with a load balancer running between the SQL Proxy and the SQL Filter Services. Details about the various deployment scenarios can be found in the system documentation.

Conclusion

Axiomatics saves time and money while decreasing risk and increasing functionality

Axiomatics is the only complete authorization solution designed to decrease the time and money spent managing access control while greatly increasing flexibility and scalability for a number of use cases and industry verticals. Thus, creating new business opportunities and ultimately better customer experiences.

By managing authorization centrally (instead of locally) and upgrading to ABAC (instead of relying soley on RBAC), Axiomatics provides fine-grained, contextually aware access to your applications, databases, or APIs so that your employees, contactors, and clients receive all of the information they do need, and none of the information they do not.

Key points in making a case for ABAC

- ABAC provides a centralized, externalized authorization management system
- ABAC can support even the most complex access control environments, to help minimize risk while allowing secure sharing of data
- Enterprises can build on Investments in RBAC systems by making roles one of the attributes in a policy-based system to move to a fine-grained approach
- Complex regulatory compliance is easily handled with a policy-based approach
- The time and cost of achieving and maintaining compliance is greatly diminished with a centralized authorization service.
- And the best news is it can be used across your environment: ABAC can be applied to applications, databases and APIs

Our best-in-class software can be deployed across any it environment to safeguard data. Call or email us to learn how Axiomatics can work with your enterprise:

AXIOMATICS

525 W Monroe St, Suite 2310
Chicago, IL 60661, USA
Tel: +1 (312) 374-3443

Västmannagatan 4
S-111 24 Stockholm, Sweden
Tel: +46 (0)8 51 510 240

info@axiomatics.com www.axiomatics.com twitter.com/axiomatics