Secure your sensitive information
Fine-Grained Access Control
Serving financial institutions, federal agencies, pharmaceutical companies, payment service providers, insurers, broadcasting companies, healthcare businesses and manufacturers around the world.
What We Do

Our solutions enable enterprises and government agencies to share and safeguard sensitive information, meet internal controls and compliance regulations, protect intellectual property and minimize data fraud. Axiomatics is the leading provider of fine-grained access control for applications, databases, big data and APIs.

Why is this necessary now?

Legacy access control models struggle to cope with cloud computing, big data, and Bring Your Own Device (BYOD) trends, and the need to meet rapidly evolving business models and new regulatory demands. Consequently, sensitive and business critical information is exposed and open to compromise.

Axiomatics’ dynamic authorization management solutions address this challenge head-on. Our industry-standard technology protects information and enables it to be securely shared across virtually any IT environment. Additionally, it enables organizations to enforce regulations and prove compliance.

How We Do It

Our product suite uses Attribute Based Access Control (ABAC) and a policy-based approach to ensure access to data is strictly controlled. To achieve this, authorization is granted or denied based on policies that reflect the unique security and compliance needs and risk appetite of the organization.

It’s not just about **WHO** can access **WHAT** information but also **WHEN**, **WHERE**, **WHY** and **HOW**
We Provide Authorization for:

**Applications**

The Axiomatics Policy Server is the leading solution for managing dynamic authorization of applications. With the fastest authorization engine on the market, we externalize the authorization process from applications to deliver secure and effective fine-grained access control.

**Data**

The Axiomatics Data Access Filter applies ABAC technology to data, thus going beyond just protecting the database container. By filtering or masking data at the source, we provide secure and effective data-centric security that ensures sensitive information is protected.

**and Big Data**

SmartGuard for Big Data is a unique solution that redacts or masks sensitive data that a user or application is not authorized to access. SmartGuard for Big Data sits between an application, such as a business intelligence tool, and intercepts access requests, and approves or denies access to data in accordance with business policies.

**We also validate and prove compliance**

The Axiomatics Review Manager enables data- and user-centric auditing of access rights. The tool allows auditors and managers to see the conditions under which a user can access data, as well the conditions under which specific data can be accessed. These unique capabilities enable organizations to prove that regulations are being complied with.
“By 2020, 70 percent of enterprises will use ABAC as the dominant mechanism to protect critical assets, up from less than 5 percent today.”  

_Gartner predicts 2014_

**A new information security paradigm for a new era**

We are now in the era of “anywhere computing”. Users expect access to information from any location at any time from any device.

Data is stored and processed in public or private clouds or in conventional in-house data centers and warehouses. Not surprisingly, the security models from pre-internet days are failing. The result: financial disasters, massive data leakage, large-scale compliance failures and inefficient business operations. A new dynamic authorization model is required to handle today’s dynamic environments: Attribute Based Access Control (ABAC).

**It’s time to adapt to the changing needs of the workplace**

Legacy authorization models, such as Role Based Access Control (RBAC), are one dimensional, and rely on a person’s role in an organization as a guide to what information can be accessed. This worked when users had one or two specific roles and there was a clear understanding of what information they should or should not be authorized to access.

However, complex authorization requirements in modern organizations often lead to an overwhelming number of overlapping roles to cater for the multitude of permissions that have to be assigned to users. Eventually administrating these roles becomes impossible. Hence the struggle many organizations face to achieve reliable segregation of duties in order to protect themselves against fraud.
Attribute Bases Access Control: The new standard for protecting data

Unlike static, single factor authorization models, Attribute Based Access Control dynamically grants or denies access to information based on multiple authorization factors and the relationship between them.

With multiple factors you can determine who can access what information and under what conditions, i.e. type of data, time of day, current location, personnel security grading or device in use. Additionally, you can control the actions an individual can carry out, such as edit or view a document, create, sign off, or view a transaction, and at what amount. Each factor is governed by your corporate policies and current regulations, rather than an individual’s role in the organization.

Cost-effective authorization management

Corporate policies are defined and centrally maintained. When a policy or regulation changes, you simply change the corresponding authorization policy and it is applied throughout your system. This eliminates the need to edit and code all the relevant applications in an IT environment every time a policy changes. This approach saves time and resources, and drastically reduces the total cost of ownership of data authorization as well as of application development and management.
Dynamic Authorization for Applications

Axiomatics provides a complete solution for dynamic authorization of applications. The Axiomatics Policy Server delivers fine-grained access control for a broad range of application environments to meet the needs of highly regulated organizations with data that needs protecting.

Most business applications are hard-coded to restrict access according to the relevant business rules at the time of design. But business rules change. Scenarios such as cross-boundary data exchange is making the process even more complex. Hard-coding applications is a static and outdated way of “securing” data and it does not scale.

The Axiomatics Policy Server

This problem can be dynamically solved with the Axiomatics Policy Server, a centrally managed decision engine that is located externally from other business applications. For every access request, an application queries the Axiomatics Policy Server to find out what users can do. The Axiomatics Policy Server, which handles requests in real-time, permits or denies access based on current rules and regulations. Additionally, as rules change, enterprises only have to update policies once and the infrastructure will remain compliant and secure across all channels and devices, whether a call is made from a traditional workstation or via mobile or cloud environments.
Advanced compliance and reporting functionality

Axiomatics Policy Server is available with the Axiomatics Review Manager tool. The Review Manager’s advanced auditing capabilities bring visibility and transparency to the authorization process. Capabilities include real-time auditing of access control from a data- and user-centric perspective. This enables an auditor, manager or architect to view the conditions under which a specific user can access certain data and the conditions under which specific data can be accessed.

- An access request is intercepted.
- A query is sent to the Axiomatics external authorization engine.
- The authorization service evaluates the relevant policies.
- It may also query external attribute sources about context data such as user clearance, information asset properties, department, location, etc.
- The decision PERMIT or DENY is returned and enforced.
Data-centric security

**Dynamic Authorization for Databases**

More people than ever before need access to data stored in databases. This however, creates security issues, as can be witnessed by high profile data leakage incidents that make global news. Many of these could be avoided with fine-grained authorization controls. Axiomatics provides dynamic authorization and dynamic data masking capabilities with the Axiomatics Data Access Filter.

**The Axiomatics Data Access Filter**

The Axiomatics Data Access Filter is a unique solution that enables you to apply dynamic authorization to databases in order to secure your data. It provides real-time filtering and masking of data at the source. By applying authorization within the data layer itself you can ensure users only have access to the details they are authorized to see and nothing else.

**Dynamic data filtering and masking**

The Axiomatics Data Access Filter intercepts database access requests and changes them on-the-fly to ensure they comply with mandated access control policies. The effect is a fine-grained filter. No data leaves the database unless the user explicitly has been duly authorized to view it. Dynamic data masking on the cell level means individual fields of a data set are redacted as mandated by a policy, for instance to protect the confidentiality of credit card or social security numbers.
Auditing and compliance

The Axiomatics Data Access Filter is available with the Review Manager component. This provides real-time reports of policies, including the conditions under which data can be viewed and the conditions that a user can view data. This enables an organization to both enforce regulations and prove compliance at the data layer.

1. An SQL statement from the application is intercepted.
2. A query is sent to the Axiomatics external authorization service.
3. The authorization service evaluates the relevant policies.
4. It may also need to query external attribute sources for more information.
5. The result is a modified SQL clause, dynamically generated according to access policies. When applied, only authorized data is returned to the user or application.
Dynamic Authorization for Big Data

With the collection of mass data, comes the security headache of safeguarding sensitive information. A smart solution is required that guards the most sensitive data but securely shares valuable data for processing to a user or application that is authorized to access it.

SmartGuard for Big Data

Axiomatics SmartGuard for Big Data resides between the data sources and an application (for instance a business intelligence tool) and intercepts data access requests. Once a request is received, it compares the conditions of the request with the conditions of the business polices and releases approved data from the data store.

Prove compliant authorization

SmartGuard for Big Data enforces business policies that reflect internal controls and regulatory compliance. When complemented with the Axiomatics Review Manager it’s possible to conduct real-time auditing of user and data access controls, and in doing so prove that regulatory compliance is met.
Dynamic data masking and redaction

SmartGuard for Big Data offers fine-grained redaction of sensitive data. Confidential data can be dynamically masked or redacted at the time of the query — and kept secure in the data store. As part of the overall policy-based approach, the choice of whether to redact or mask will depend on the use-case and type of information being stored and processed.

- An access request from the application is intercepted.
- A SQL query is sent to the Axiomatics SQL Transformer.
- The SQL transformer modifies the statement based on what the user is allowed to access.
- It also may need to query other attribute sources for more information.
- A modified SQL statement is returned to the Interceptor. Access to the right data, under the right conditions, is then granted.
Facilitate enhanced e-services to customers by securing data access in a new customer portal for Switzerland’s largest health insurer.

Enforce export control policies and protect IP at a leading global helicopter manufacturer, with dynamic PLM and manufacturing data access control.

Support real-time authorization of hundreds of millions of users and daily transactions, at one of the world’s largest online payment service providers.
Streamline the access request management joiner/mover/leaver process by enforcing fine-grained access controls at the world’s largest re-insurer.

Safeguard confidential data from insider threats with Attribute Based Access Control to control access based on policies that scale and adapt.

Enable data from highly classified clinical trials to be securely shared among stakeholders at a global pharmaceutical company with the Axiomatics advanced database masking/filtering service.