AXIOMATIC DATA ACCESS FILTER MD
Attribute Based Access Control for Databases

Benefits

- Provides context-aware authorization to data with attribute-based access control policies
- Real-time, dynamic filtering of data
  Denies access to data that a user is unauthorized to access
- Real-time, dynamic data masking
  Masks individual cell values such as credit card or social security numbers
- Real-time unmasking of data
  Transforms data if user is authorized, for instance to decrypt an encrypted field
- Changes in business rules are made once and applied centrally rather than on each database or application
- Axiomatics Data Access Filter MD supports multiple database types:
  - Oracle
  - IBM DB2
  - Microsoft SQL Server
  - Teradata

Inefficient use of data impedes productivity and revenue growth

Studies show that data usability directly impacts productivity and revenue. Usability, in this context, means making information easily available to users without jeopardizing data integrity and confidentiality as mandated by business rules and regulations. One study¹ claims only 10% usability increase translates to a median increase of over $2 billion in total annual revenue among Fortune 1000 companies, or almost $56,000 in additional sales per employee.

Yet, in spite of obvious benefits, many organizations fail in their attempts to improve their use of data. Why?

The answer, in a word, is security. Sensitive data must be protected against unauthorized access. Exposing your information systems to new types of cloud services, new mobile or remote users and new BI tools without taking adequate security precautions, leads to information leakage, fraud risks, privacy breaches, intellectual property exposure, or regulatory compliance violations.

Data-centric security unlocks revenue streams and increases productivity

The Axiomatics Data Access Filter MD delivers fine-grained database protection by enforcing organizational policies using rich Attribute Based Access Control (ABAC) policies. Policies consider who the user is, what data the user is requesting, when and how it is done and in what context.

Through database activity monitoring every single database query made by users in the organization is controlled. Queries that would return data sets which in any way violate policies are altered on the fly to redact or mask sensitive information. Data never leaves the database unless the user has adequate authorization. Furthermore, using data unmasking you can also pre-process data for authorized users, for instance to decrypt cell-values which are stored encrypted in the database.

Once data security is assured, users can access data via new types of channels and services to securely share information. New and more efficient business processes can then be implemented to increase productivity.

¹"Measuring the Business Impacts of Effective Data", study made at University of Texas and Indian School of Business
### Beyond dynamic data masking and database activity monitoring

This example illustrates the effects of policy controlled data access filtering and data masking. The HR database holds information about employees.

A corporate policy mandates that department managers can view data about employees in their own department only. Data access filtering leaves the manager of dept D with this data set:

<table>
<thead>
<tr>
<th>Name</th>
<th>Salary</th>
<th>Dept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Velma Lapointe</td>
<td>123 456</td>
<td>A</td>
</tr>
<tr>
<td>Antonio Wagstaff</td>
<td>134 567</td>
<td>B</td>
</tr>
<tr>
<td>Susie Wooley</td>
<td>187 344</td>
<td>D</td>
</tr>
<tr>
<td>Sheri Albanese</td>
<td>146 743</td>
<td>B</td>
</tr>
<tr>
<td>Ronald Fulton</td>
<td>169 438</td>
<td>A</td>
</tr>
<tr>
<td>Jennifer Washburn</td>
<td>174 345</td>
<td>D</td>
</tr>
</tbody>
</table>

The policy is changed to state that only the salary information is sensitive and needs to be hidden. According to the new policy, managers can see all employee records but only the salaries of people within their own departments. With data masking applied to the salary column, department managers see all employee records but only salary data for their direct reports.

<table>
<thead>
<tr>
<th>Name</th>
<th>Salary</th>
<th>Dept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Velma Lapointe</td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Antonio Wagstaff</td>
<td></td>
<td>B</td>
</tr>
<tr>
<td>Susie Wooley</td>
<td>187 344</td>
<td>D</td>
</tr>
<tr>
<td>Sheri Albanese</td>
<td></td>
<td>B</td>
</tr>
<tr>
<td>Ronald Fulton</td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Jennifer Washburn</td>
<td>174 345</td>
<td>D</td>
</tr>
</tbody>
</table>

Note that the policy change requires no change in the HR application or database.

### Documented use case

The white paper *Increasing the Value of Information with Fine Grained Security for Data Marts* on the Axiomatics website describes a use case in detail. The authors handle clinical research data. The information is both privacy-sensitive and IP-sensitive and can only be made available under very specific conditions.

An example of a business rule that must be enforced looks something like this: *Access to data relating to an unpublished clinical trial is only granted to members of the associated development team or to managers above level X.*

This query is used as an example:

```
Select patient_count from Clinical_Trial
```

If the user is a member of development team ‘ABC’ but not a manager above level X, the Axiomatics Data Access Filter alters this query on-the-fly to:

```
Select patient_count from Clinical_Trial where study="ABC"
```

1 White paper download available from here: [http://www.axiomatics.com/resources.html](http://www.axiomatics.com/resources.html)