SmartGuard™ for Big Data 1.0

Introducing SmartGuard™ for Big Data from Axiomatics

SmartGuard™ for Big Data from Axiomatics is the only Big Data authorization solution that supports the full capability and delivers the true flexibility of Attribute Based Access Control (ABAC). It protects big data systems against unauthorized access and exfiltration of data; only allowing authorized users or applications to access the data they are entitled to, in accordance with corporate policies. The smart solution enforces access based on multiple categories of attributes, and the relationship between them. This includes data classification, purpose of use, time of day, user location, device in use, and the user's role or group. In addition, SmartGuard for Big Data can dynamically mask or redact data at the time the query is run, combining filtering and masking in a single, powerful solution.

Key Features

- Enables fine-grained authorization for big data
- Exploits the full power of additional attribute lookup from multiple attribute sources
- Redacts and masks sensitive data, such as credit card numbers, for unauthorized users
- Automates modification of SQL statements to control what data will be retrieved with dynamic data filtering
- Transform cell values for an authorized user, using native functions or external services (e.g decryption)
- Facilitates the creation and testing of standards-based policies that are XACML 3.0-conformant

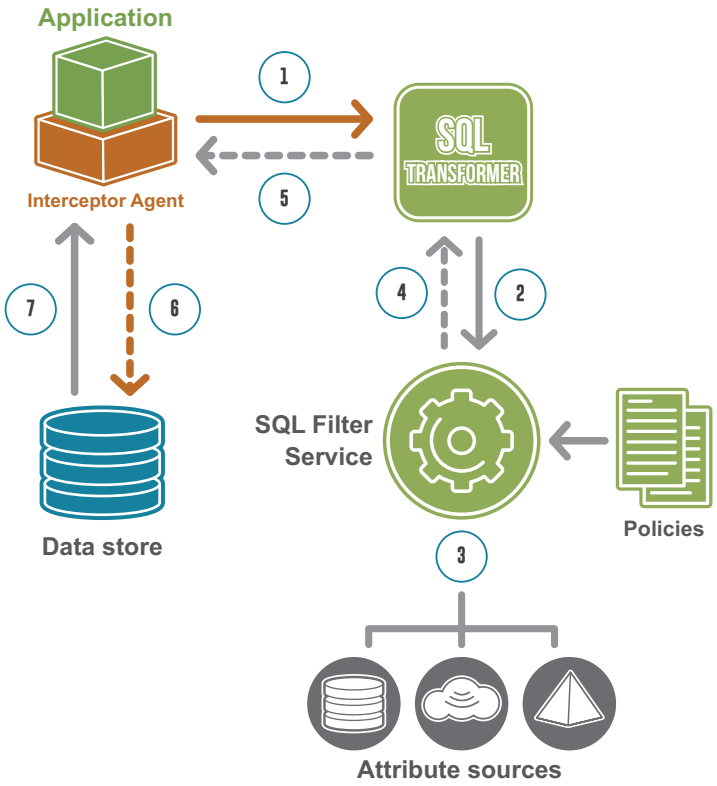
How Does it Work?

When an application sends a data access request, the SQL query is intercepted and sent to the SQL Transformer. The SQL Transformer modifies the query according to authorization policies that govern access rights. These are based on contextual information about the user, the data being accessed and other related attributes. Rich attribute sources may be queried for more information on the context of the policy evaluation. A modified access-control-enhanced SQL query is returned to the interceptor. This modified query is then sent to the data store and access to the right data, under the right conditions is provided.

Explore, Validate, and Certify Standards-Based Access Policies

SmartGuard for Big Data provides fine-grained access control from Java-based and .NET-based applications for HAWQ, a Hadoop Native SQL Database. Data that the user is not authorized to access is filtered out.

- Policy-driven data access filtering as well as dynamic data masking and unmasking of database contents
- Centralized policy management and advanced auditing capabilities
- Protection of Big Data stores



SmartGuard for Big Data 1.0 Specifications

Operating environments

- SQL Transformer
  - Windows Server 2008, 2008 R2, 2012, 2012 R2
  - Redhat Enterprise Linux 5.3+ and 6.1+
- SQL Filter Service:
  - Windows Server 2008, 2008 R2, 2012, 2012 R2
  - Redhat Enterprise Linux 5.3+ and 6.1+
- APS Express Edition:
  - Redhat Enterprise Linux 5.3+, 6
  - Windows Server 2008 R2, 2012

Java environments

- Oracle JDK 7, 64-bit
- Oracle JDK 8, 64-bit

Disk and memory

- SQL Transformer
  - Minimum memory: 2 GB (256 MB for the managmenet console running standalone)
  - Minimum disk space: 3 GB
- SQL Filter Service:
  - Minimum memory: 2GB
  - Minimum disk space: 100 MB
- APS Express Edition:
  - Minimum memory: 2 GB
  - Minimum disk space: 1 GB

Supported data stores

- HAWQ, a Hadoop Native SQL Database.
- SmartGuard for Big Data has been tested with HAWQ 2.0.0.

Supported applications

- Java-based application, Java 7 is supported
- .NET-based application using an ODBC connection (Windows 7, Windows Server 2008, or Windows Server 2008 R2)

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

webinfo@axiomatics.com www.axiomatics.com twitter.com/axiomatics