AXIOMATICS

DATA SHEET

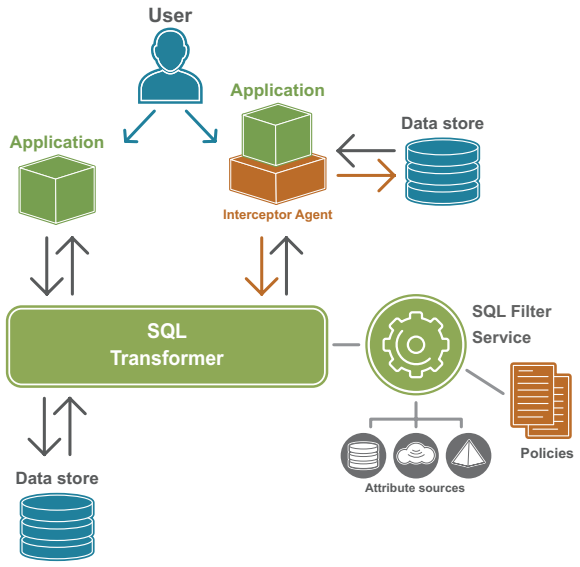
SMARTGUARD® FOR BIG DATA

SMARTGUARD® FOR BIG DATA FROM AXIOMATICS

SmartGuard for Big Data from Axiomatics protects big data stores against unauthorized access and exfiltration of data; only allowing authorized users or applications to access the data they're authorized to see, at the right time, under the right conditions. This ensures the most critical assets are protected against nefarious activity, and that secure collaboration can take place to speed time to market and fully realize the power of the data set. SmartGuard for Big Data also provides dynamic data masking and redaction in a single, powerful solution.

KEY FEATURES

- Delivers fine-grained authorization for Big Data SQL-on-Hadoop engines Apache Impala, Hive and HAWQ
- 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
- Transforms 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
- Compatible with Axiomatics Policy Server
- Exploits the full power of additional attribute lookup from multiple attribute sources



HOW DOES IT WORK?

SmartGuard for Big Data operates by modifying SQL queries so that their execution always respects the conditions stated in the access control policy. This can be done via two different deployment models (which can coexist): Using the SQL Transformer as a proxy, or using an Interceptor Agent.

In both cases, the user makes a request for access to the Big Data store through an application that sends it to the SQL Transformer, which, through the SQL Filter Service, changes it in real time, based on user entitlements as defined by corporate policies.

If the SQL Transformer is used as a proxy, the modified query is forwarded directly to the data store, after which the authorized data set is returned to the user.

If the Interceptor Agent model is used, the Interceptor Agent intercepts the SQL statements from the application before sending them to the SQL Transformer. The modified query is sent back to the Interceptor Agent and then allowed to proceed to the data store for execution. The authorized data set is then returned to the user.

EXPLORE, VALIDATE, AND CERTIFY STANDARDS-BASED ACCESS POLICIES

SmartGuard for Big Data provides fine-grained access control for data stored in Hadoop through the SQL-on-Hadoop engines Impala, Hive and HAWQ.

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

SMARTGUARD FOR BIG DATA 1.3 SPECIFICATIONS

SUPPORTED DATA STORES

- Hadoop through the SQL-on-Hadoop engine Hive version 1.1 and above. SmartGuard for Big Data has been tested with Cloudera Distributed Hadoop (CDH) 5.7.6.
- Hadoop through the SQL-on-Hadoop engine Impala version 2.5.0 and above. SmartGuard for Big Data has been tested with Cloudera Distributed Hadoop (CDH) 5.7.6 and 5.12.1.
- Hadoop through the SQL-on-Hadoop engine HAWQ. SmartGuard for Big Data has been tested with HAWQ 2.0.0 on Hadoop 2.7.2.

SUPPORTED APPLICATIONS WITH INTERCEPTOR AGENT DEPLOYMENT

- Java-based application, Java 7 and 8 are supported
- Windows-based application using an ODBC connection (Windows 7, Windiws 10, Windows Server 2008 R2, or Windows Server 2012 R2)

JAVA ENVIRONMENTS

- Oracle JRE 8, 64-bit
- Oracle JDK 8, 64-bit

WEB BROWSERS

- Firefox 52.0 ESR or later
- Chrome 51.x or later
- EdgeHTML 15 or later
- Internet Explorer 11

SUPPORTED JDBC DRIVERS

- All main JDBC drivers for Hive (from Cloudera and Hortonworks), Impala (Cloudera) and HAWQ (Postgres and DataDirect Greenplum).

SUPPORTED ODBC DRIVERS

- Selected ODBC drivers for Hive (from Microsoft, Cloudera and Hortonworks), Impala (Cloudera) and HAWQ (Postgres).

OPERATING ENVIRONMENTS

SQL Transformer:

- Windows Server 2008 R2, 2012 R2
- Redhat Enterprise Linux 7.3, 7.4

SQL Filter Service:

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Redhat Enterprise Linux 5, 6, 7 with latest updates

APS Express Edition:

- Windows Server 2008 R2, 2012, 2012 R2
- Redhat Enterprise Linux 5, 6, 7
- CentOS 5, 6, 7
- Ubuntu Server 12.04 LTS, 14.04 LTS, 16.04 LTS
- SUSE Linux Enterprise Server 11, 12

DISK AND MEMORY

SQL Transformer:

- Minimum memory: 2 GB (256 MB for the management console running standalone)
- Minimum disk space: 3 GB

SQL Filter Service:

- Minimum memory: 2GB
- Minimum disk space: 100 MB

APS Express Edition:

- Hardware x86-64 CPU
- Minimum: 2 GB (4 GB recommended)
- Minimum: 900 MB (2 GB recommended)

SECURITY

- Secure communication between the application and SQL Transformer and between SQL Transformer and the database using TLS

USER AUTHENTICATION

- Kerberos and LDAP/Active Directory

WWW.AXIOMATICS.COM | WEBINFO@AXIOMATICS.COM

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

11921 Freedom Drive
Two Fountain Square, Suite 550
Reston, VA 20190, USA
+1 (703) 943-0747
sales@axiomaticsfederal.com

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