

# SMARTGUARD® FOR DATA

## SPARK SQL EDITION

### SMARTGUARD® FOR DATA - SPARK SQL EDITION

SmartGuard for Data protects big data stores against unauthorized access and exfiltration of data; only allowing 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 unauthorized activity, enabling secure collaboration, speeding time to market and fully realizing the power of the data set. SmartGuard for Data provides dynamic data masking, filtering and redaction in a single, powerful solution.

### BENEFITS

- **Provides** data-centric security for Apache Spark™, a unified analytics engine for large-scale data processing
- **Enables** fine-grained authorization wherever Apache Spark is installed - in the cloud or on-premise with Databricks, AWS, Azure, Cloudera
- **Enables** secure collaboration and data sharing
- **Provides** visibility and control of authorization policies, as well as ease of audit
- **Provides** dynamic data masking and data filtering, down to the row and cell level
- **Enforces** access control for critical assets and intellectual property
- **Centralizes** efficient management of authorization and permissions management, saving time and money
- **Increases** "speed to data" and does not impede analytics
- **Mitigates** risk of data access, enabling collaboration to find value in data, monetize it and market it securely
- **Helps** achieve complex regulatory compliance, such as privacy regulations like GDPR
- **Delivers** standards-compliant Attribute Based Access Control protection

### SMARTGUARD FOR DATA

With the shift to using large data stores also comes the responsibility to secure them. This challenge is often the responsibility of the CSO/ CISO and the security department, or even individual project teams. Whether a data project is in the planning stages, or already in motion, these teams must ensure that sensitive information is safeguarded and regulatory compliance is met, while not impeding the speed of business or analytics processes. SmartGuard for Data - Spark SQL Edition extends Axiomatics' leading data authorization suite to structured data in Apache Spark.

### SECURELY SHARING DATA

SmartGuard for Data Spark SQL edition provides a layer of fine-grained authorization for Apache Spark, to ensure privacy, data access governance and speed-to-data. Data processing platforms such as Databricks, Qubole, Google BigQuery, etc. can use SmartGuard Spark SQL edition to seamlessly control access for any processing task in real-time, regardless of where the data resides - it could be in any Apache Spark implementation, such as GCP Dataproc, AWS EMR, Azure HDInsight or Cloudera.

For data analytics platforms like Databricks, SmartGuard for Data works seamlessly to help protect the data that flows through the platform. For orchestration tools like Kubernetes, SmartGuard for Data is easily deployed and works seamlessly within these workflows.

Use cases for SmartGuard for Data include secure data sharing for pharmaceuticals, life sciences, banking, healthcare, manufacturing and more. This latest innovation expands the industry-leading Axiomatics Dynamic Authorization Suite, protecting applications, data, APIs and Microservices.



### CUSTOMER INNOVATION

A large international pharmaceutical company is using Smartguard for Data in a revolutionary way. Their vision is to share massive research data stores with the global research, healthcare and medical communities. Policy-based fine-grained access control enables this secure sharing, and allows for the right people to have access to the right data. In expanding access to the global healthcare community, the company foresees a new caliber of collaboration - fueling new insights to healthcare, new drugs and a healthier world population.

## ATTRIBUTE BASED ACCESS CONTROL: THE KEY TO SECURELY SHARING DATA

Unique in its attribute-based policy approach to access management, SmartGuard for Data provides control and visibility of user access to large data stores either on-premise or in the cloud. By leveraging Attribute Based Access Control (ABAC), enterprises can quickly share sensitive data, fueling collaboration, speed to market and new innovation, while also ensuring privacy and intellectual property are secured. Attributes are used to create access control policies for queries through data analytics applications to the SQL analytics engine Spark SQL. SmartGuard for Data offers the next generation of dynamic and policy-based authorization, with a wide range of benefits that enable sensitive data to be securely shared on premises, via the cloud, with third parties, and across multiple devices.

## VISIBILITY AND CONTROL

Access control policies can detail what data (at the granularity of row and cell level) can be accessed by whom, and the conditions under which the data can be accessed. Furthermore, using attributes to build policies means the possibilities for control are endless. Ease of user configuration is improved through a modern SQL Filter Service Configuration GUI, which also augments visibility and control thanks to the ability to apply ABAC on the configuration GUI itself, creating policies to ensure that configuration and policy tasks are assigned with fine-grained policies. Configurations can also be managed through easy-to-use RESTful APIs.

## SAVE TIME AND MONEY

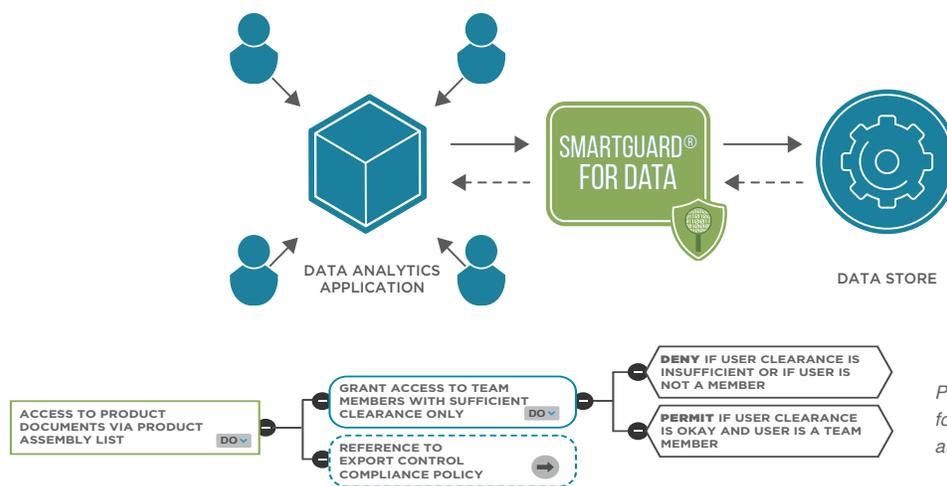
Centralized management means huge savings of time and developer resources, as all ABAC policies are externally managed rather than hard coded into individual applications, business tools or backend systems. This makes changing user permissions fast and cost effective. They can be easily changed once and applied across the enterprise so businesses can respond quickly when regulations, internal policies or supplier agreements change. SmartGuard has access to the Axiomatics Policy Server's industry-leading graphical user interface for writing and managing policies.

## SECURITY AND USER AUTHENTICATION

SmartGuard for Data respects best practices for security, including cloud deployments, and supports secure communication between the data analytics application, SQL Transformer and the Spark SQL engine using TLS. User authentication can be managed with out-of-the-box Apache Spark username+password, or via LDAP/Active Directory.

## SECURE NEW AND EXISTING DATA DEPLOYMENTS

Whether your organization is looking to secure access to new or existing Spark SQL implementations, it's straightforward to get started with SmartGuard for Data from Axiomatics.



*Policies are the power in SmartGuard for Data, delivering fine-grained authorization in real-time.*

Would you like more information on SmartGuard for Data? Contact your sales representative or email us at: [webinfo@axiomatics.com](mailto:webinfo@axiomatics.com).

[WWW.AXIOMATICS.COM](http://WWW.AXIOMATICS.COM) | [WEBINFO@AXIOMATICS.COM](mailto:WEBINFO@AXIOMATICS.COM)

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

42395 Ryan Rd  
Suite 112 - PB Box 805  
Brambleton, VA 20148  
+1 (801) 556-9994  
[sales@axiomaticsfederal.com](mailto:sales@axiomaticsfederal.com)

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

