SMARTGUARD® FOR BIG DATA
SECURELY SHARE YOUR INFORMATION ASSETS

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.

BENEFITS

- **Provides** data-centric security for SQL-on-Hadoop engines Apache Impala, Hive and HAWQ

- **Delivers** standards-compliant Attribute Based Access Control protection

- **Provides** visibility and control of authorization policies

- **Enables** secure collaboration

- **Provides** dynamic data masking and data filtering

- **Enforces** access control for critical assets and intellectual property

- **Protects** data at row and cell level

- **Transforms** cell values for an authorized user, using native functions or external services (e.g decryption)

- **Helps** achieve complex regulatory compliance, such as GDPR

SMARTGUARD FOR BIG DATA

Big Data has changed the way many large organizations operate. Enterprises are now the custodians of increasing amounts of business and customer data as more and more information is gathered from applications, services, and the Internet of Things (IoT). For example, there is an influx of data transmitted from connected devices that report on product performance and personal usage. Big Data such as this has to be stored, processed, shared and analyzed to realize its true value, to leverage insights, and to meet business objectives, such as improve product performance or the service offering.

With the shift to using Big 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 big 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 business or analytics processes.

SAFELY SHARING BIG DATA

In practice, Big Data is used to help meet business objectives that often focus on bringing better products to market or streamlining customer service. Sophisticated analysis on Big Data fuels an understanding of customer needs and trends, operational improvement opportunities, design upgrades (often using data that feeds back from products, devices or interaction points), and so on: all leading to better products and an improvement in customer care and satisfaction.

These objectives stem from the ability to get to timely and key insights in the data. This requires sharing across business units up and down the org chart and with trusted third parties. Information sharing is necessary - but at the same time there should be focus is on the protection of critical assets, data and PII that is stored within these large data sets.

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

SmartGuard for Big Data uses Attribute Based Access Control (ABAC) principles to create access control policies for organizations that run SQL-based queries on Hadoop through SQL-on-Hadoop engines Impala, Hive and HAWQ. ABAC 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 augment visibility and control thanks to the ability to apply ABAC on the SmartGuard configuration console 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.
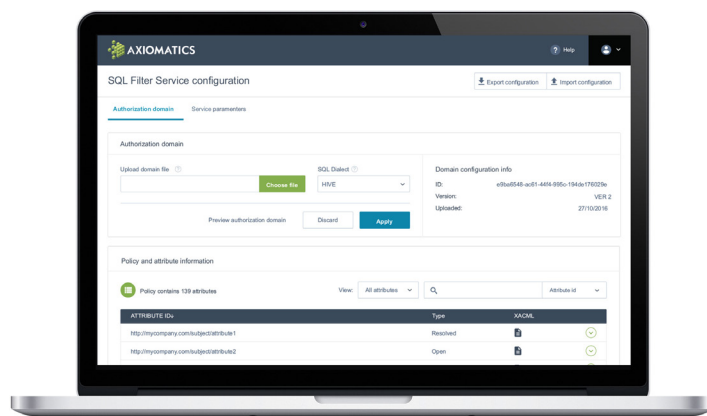
The SQL Filter Service Configuration GUI for SmartGuard

SECURITY AND USER AUTHENTICATION

SmartGuard for Big Data respects best practices for Hadoop security, including cloud deployments, and supports secure communication between the application, SQL Transformer and the database using TLS. User authentication can be managed via Kerberos and LDAP/Active Directory.

SECURE NEW AND EXISTING BIG DATA DEPLOYMENTS

Whether your organization is looking to secure access to new or existing Hadoop Big Data implementations, it's straightforward to get started with SmartGuard for Big Data from Axiomatics. We can help you meet your evolving security and information sharing needs as your use of Big Data expands.

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

WWW.AXIOMATICS.COM | WEBINFO@AXIOMATICS.COM