

# SmartGuard™ for Big Data

## Securely Share your Information Assets

### SmartGuard™ for Big Data

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.

### Benefits

- **Provides** data-centric security for Hadoop
- **Delivers** standards-compliant Attribute Based Access Control protection
- **Provides** visibility and control of authorization policies
- **Enables** secure third-party collaboration
- **Provides** dynamic data masking and data filtering
- **Enforces** access control for critical assets and intellectual property
- **Protects** data at row and cell level
- **Transform** cell values for an authorized user, using native functions or external services (e.g decryption)



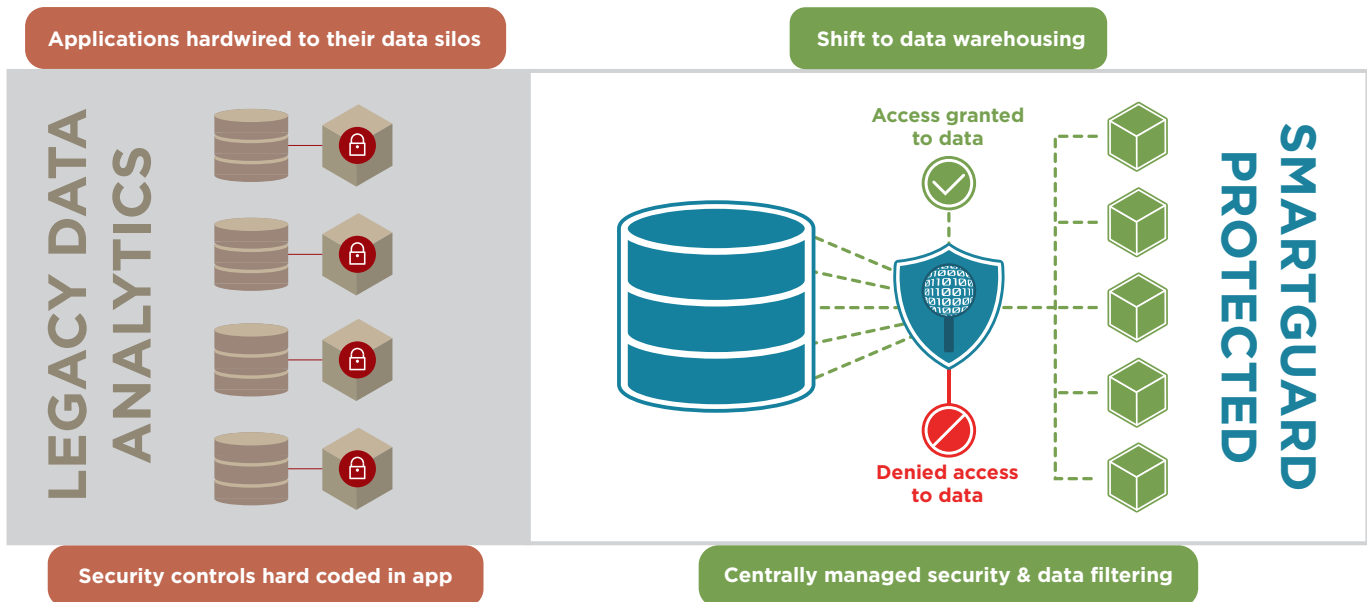
### Introducing SmartGuard™ for Big Data from Axiomatics

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 compliance/regulations are 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.



For stakeholders in the Big Data analysis, liberation and monetization workflows, utilizing ABAC means that their work remains seamless. Authorization for individual users, based on context, conditions and internal policies is enforced at new layers outside the tools at the time data is requested from a Big Data store.

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

To meet this challenge head-on, Axiomatics introduces SmartGuard for Big Data. It uses Attribute Based Access Control (ABAC) principles to create access control policies for organizations that run SQL-based queries on Hadoop. ABAC offers the next generation of dynamic and policy-based authorization. It offers organizations 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. Visibility and control are further enhanced thanks to centralized management of policies.

### 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. A business-friendly graphical user interface means high-level expression of policies, and the ability to create very rich, context-aware policies on the fly.

### Secure New and Existing Big Data Deployments

Even though many of these Big Data implementations are already in motion, organizations can easily implement a layer of smart data access control with dynamic authorization from Axiomatics.

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