IMPERVA®

Imperva SecureSphere Agent for Big Data

DATASHEET

Meet Security and Compliance Audit Requirements on Big Data

Protects Big Data Deployments

The sensitive data stored in Big Data deployments is subject to the same compliance requirements as sensitive data in databases and it must also be protected from data breaches and unauthorized access. SecureSphere Agent for Big Data provides security, audit and risk professionals with real-time visibility into data usage in Big Data deployments. The enhanced visibility and reporting capabilities improve data security and aid in meeting compliance directives.

SecureSphere Agent for Big Data provides security, audit and risk professionals with real-time visibility into data usage in Big Data deployments

Audit Scale and Performance at Big Data Levels

Most Big Data audit solutions were not built to scale with the high volume, velocity, and variety of sensitive data stored within Big Data environments. The SecureSphere Agent for Big Data is designed to avoid scalability pitfalls, by monitoring activities directly from within Big Data components. Only the relevant audit data is sent to the Gateway further minimizing impact on bandwidth, storage, and subsequent analysis. More relevant data, transported efficiently, optimally stored and available in real-time provide a highly scalable model for enterprise data security and compliance processes.

SecureSphere Agent for Big Data Benefits

- Gain visibility into privileged users, and unusual or abnormal activities
- Meet compliance requirements for sensitive data in Big Data repositories
- Accelerate incident response and forensic investigations
- Protect sensitive data in Big Data deployments

Extends Uniform Activity Monitoring to Big Data

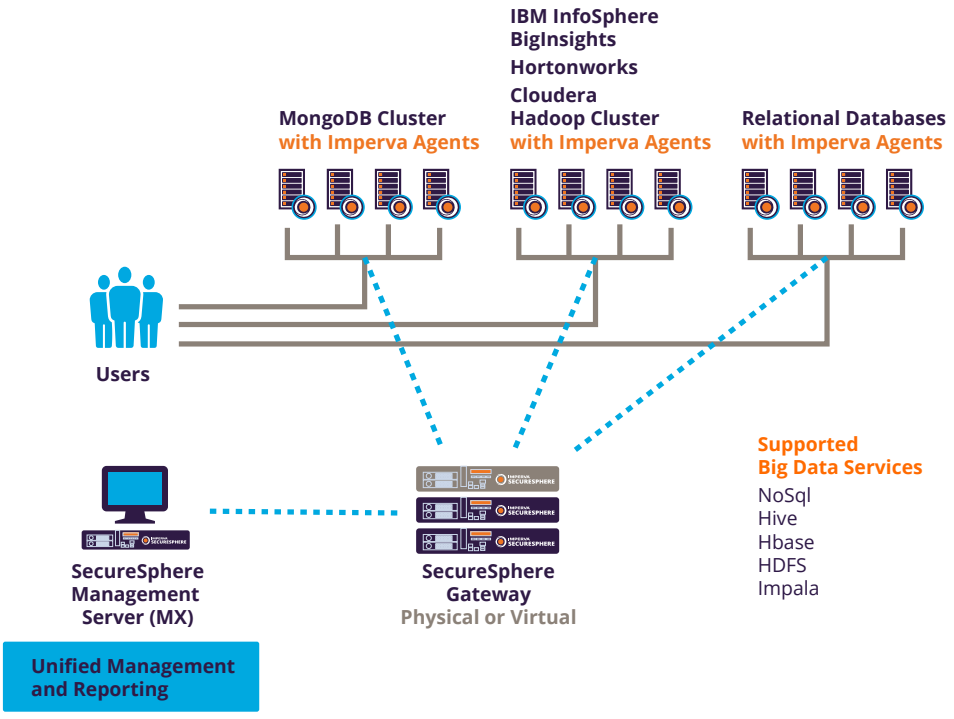
The SecureSphere Database Activity Monitoring solution utilizes a logical abstraction layer that enables the application of SecureSphere database policies to Big Data nodes with no requirement to alter the policy rules into specific Big Data languages. This ensures audit data from monitored Big Data nodes is processed and shown with audit data from other enterprise systems, providing a complete, unified view of access to sensitive data. The SecureSphere dashboard views, reports, and alerts accelerate incident response and enable quick resolution across both databases and Big Data repositories.

Minimizes the need for Big Data expertise

The SecureSphere Management Server provides an easy to use policy definition and management that applies policies uniformly across all types of data stores. The SecureSphere Agent for Big Data automatically translates policy rules into the specific language used by each supported Big Data service. The agent automatically filters out non-relevant information in real-time, sending only the requested audit information to the Gateway.

Within the Big Data environment, there is no universal equivalent to the SQL language used on databases. In addition, a simple command to "read" a Big Data record is broken down into many smaller transactions. Manual development of audit policies would require expertise in each Big Data command language and a precise understanding of what low-level commands constituted each type of activity to be monitored. Then this would need to be rolled up into synchronized policies that matched those applied to the databases. Inevitably this model would lead to errors and eventually the audit process would be stopped, leaving the the company with no audit for compliance purposes, and the Big Data would be unprotected.

By automatic translation of policy rules into repository - specific commands - SecureSphere Agents for Big Data eliminate the need to develop and maintain an expertise in the Big Data services being audited.



Imperva SecureSphere Cyber Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere Web, Database and File Security. It scales to meet the data center security demands of even the largest organizations, and is backed by Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

Detect Unauthorized Access and Fraudulent Activity

Gain visibility into privileged user activity, and suspicious or unauthorized access activity on Big Data repositories. When abnormal or unacceptable access activity is detected, SecureSphere triggers alerts in real-time. To streamline business processes, alerts can be sent to administrators, Security Information Event Managers (SIEM), ticketing systems, and other third-party solutions.

Accelerate, Security Investigations and Forensic Analysis

SecureSphere simplifies compliance reporting and forensic investigations, and identifies trends and patterns that indicate security risks. The SecureSphere interactive analytics dashboard provides deep insight into audited activities, and enables security teams and auditors to view, analyze, and correlate data activities using an intuitive user interface that does not require scripting. For companies utilizing Splunk for advanced analysis there is a dedicated interface panel with predefined data placeholders, a dedicated API set and a free pre-built activity analysis dashboard and report app on Splunkbase.

Real-Time Architecture

SecureSphere collects and analyzes database and Big Data activities in real-time, and instantly notifies security and operations teams about any violation of corporate data access policies. The agent architecture easily scales to meet the most demanding environments, with each SecureSphere appliance capable of supporting multiple agents and scaling horizontally to meet even the largest and most complex database and Big Data environment needs.