NEXTLABS®

Data Access Enforcer

DATASHEET

Data Access Enforcer for BigQuery

THE SITUATION

A cloud data warehouse (CDW) is a system, which uses the space and compute power allocated by a cloud provider to integrate and store data from disparate data sources. It is employed for data structured storage, analysis and reporting.

As more and more enterprises move to the cloud, they are abandoning their legacy on-premise data warehousing technologies, including Hadoop, for these new cloud data platforms. The need to meet security and compliance requirements becomes that much more important. As a result, organizations today need solutions that can secure the structured data manage by CDW.

THE SOLUTION

NextLabs Data Access Enforcer for BigQuery (DAE for BigQuery) enables you to secure your valuable data in BigQuery. The solution leverages user and host attributes in making access decisions. At the end of the day, DAE for BigQuery simplifies the design and development of security features into your application.

Key capabilities include:

- Granular controls over filtered rows in BigQuery tables
- Granular controls over specific actions in BigQuery databases

THE BENEFITS

DAE for BigQuery provides the following benefits:

- Externalize authorization management to simplify and reduce the time spent on administering access control policies
- React more rapidly to changes in business requirements, market conditions, or regulatory environment since policy changes can be made without requiring code changes or application downtime
- Lower your total cost of ownership as you can leverage your existing investment in the NextLabs platform
- Reduce the cost of compliance through more efficient and cost-effective monitoring and audit of your data

KEY FEATURES

Feature	Detail
Filtering controls	- Control what users can do with filtered rows in BigQuery tables - Filter the database rows by operation (e.g., Select, Update, Delete) such that users cannot select, update, or delete rows that have been filtered
Block controls	- Control whether users can block certain actions - Block by operation (e.g., Insert, Call) such that users cannot insert a base table or call a stored procedure
Mask control	- Mask and block user to update confidential data

SUPPORT INFORMATION

API	jobs.query jobs.insert tabledata.insertAll tabledata.list
Google Platform	APIGEE & Google Kubernetes Engine (GKE)
DB	BigQuery
NextLabs Platform	Control Center 9.1, Java Policy Controller 9.1 Control Center 2020.04, Java Policy Controller 2020.04

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS®