NEXTLABS®

Data Access Enforcer for PostgreSQL

Control Global Data Access from Anywhere

OVERVIEW

PostgreSQL is a powerful, open source object-relational database system with over 35 years of active development that has earned it a strong reputation for reliability, feature robustness, and performance.

With so many applications and business functions depending on PostgreSQL databases, it is critical that the access to those databases is controlled and secure. This is made challenging by the wide variety of data that is stored in the databases, as well as the number of users and systems that depend on accessing that data. Organizations need solutions to secure the data in their PostgreSQL databases that are both scalable and sophisticated enough to handle those security challenges.

THE SOLUTION

NextLabs Data Access Enforcer for PostgreSQL (DAE for PostgreSQL) provides dynamic data-level security controls and fine-grained data access governance for PostgreSQL by serving as a database proxy, allowing all calls from ODBC/JDBC or any library's Client to a PostgreSQL Database to be evaluated against DAE's data access policies. Through NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policy and centralized policy management to improve their security and compliance posture for PostgreSQL. DAE for PostgreSQL enforces data-level security controls - such as field-level data masking and record level data segregation and monitors data access activity directly from within the data access layer where calls are made to the ODBC interface.

DAE for PostgreSQL prevents unauthorized access to sensitive data through fine-grained data-level security controls, protecting data and addressing compliance requirements at the same time. DAE for PostgreSQL enables employees and external partners to share critical information and collaborate in business processes to improve workforce productivity and business agility.

DAE for PostgreSQL leverages user and host attributes in making access decisions, simplifying the design and development of security features into your application.

THE BENEFITS

DAE for PostgreSQL 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 with policy changes that can be made without code changes or application downtime
- Lower your total cost of ownership by leveraging your existing investment in the NextLabs platform
- Reduce the cost of compliance through more efficient and cost-effective monitoring and auditing of your data

Key Features

Feature	Detail
Real-time enforcement of attribute-based access policies	Access to data based on policies that examine attributes of data being accessed, context of requests, and user identity. DAE dynamically applies policies, factoring in changes in attributes of data or user to enforce fine-grained entitlement and security controls to data regardless of business transaction. Rules are validated in real-time when a user attempts to access data, then granting access.
Field-Level Data Masking	Given the growing importance of data privacy and the various requirements mandating the protection of sensitive data, such as personally identifiable information (PII), customer data, technical data, financial data, etc., the need for data masking is as crucial as ever. DAE ensures that users can only view the fields on the record to which they have been granted access, the value of the field will be masked for those fields that users are not authorized. It uses policy-driven approach to mask the data in the unauthorized fields based on attributes. These centrally manage policies define masking patterns and rules to determine who, what, when, where, and why to mask field(s) in real-time.
Format Preserving Encryption (FPE) Data Masking	Elements in the DB data store can be masked at rest such that the masked data preserves the length and format of the original data, making the masking non-obvious to unauthorized users and maintaining application dependencies. Masking can be reversed to allow authorized users to view the original data. DAE for PostgreSQL includes a built-in FPE library or can integrate with 3rd party encryption tools. DAE's Bulk Obfuscation Tool (BOT) makes applying FPE masking at rest consistent and straightforward across all affected tables and fields pre- and post-implementation of DAE.
Record-level Data Segregation and Filtering	DAE ensures users can only view records or data to which they have been granted access. Authorization can be based on the industry, location, department, position, project assignment, or any attribute of the user, which can be compared against attributes of an entity or record such as sensitivity, transaction type, etc. For example, you can filter data returned in a SQL query to only include records that are authorized to be accessed in the geography where the query originated.
Granular DML actions	Block by operation (e.g., Insert, Delete) such that users cannot insert a record into a table or delete a record from a table if they are not authorized to do so.
Centrally Managed Policies	Authorization policies can be centrally managed and reviewed across all an organization's applications, substantially reducing administration costs.
Centralized Monitoring and Auditing	DAE tracks and stores user activities and data access across all applications in a central audit server, simplifying compliance management. Analytics for user behavior and access patterns are provided via dashboards, reports, and automated monitoring facilities.
Out of the Box Integration	DAE serves as a database proxy, allowing all applications that connect to a PostgreSQL database to use DAE without any custom code required.

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust 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, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.