NEXTLABS®

Data Access Enforcer

Data Access Enforcer for Oracle

THE SITUATION

Oracle databases have long powered many enterprises applications and backend systems. Although Oracle has many software products and lines of business, databases are still the first thing most people think of when they hear Oracle. Oracle databases are often accessed remotely using Oracle Client software that connects to database servers using Oracle's SQL*Net.

With so many applications and business functions depending on Oracle databases, it is critical that the remote 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 Oracle databases that are both scalable and sophisticated enough to handle those security challenges.

THE SOLUTION

NextLabs Data Access Enforcer for Oracle (DAE for Oracle) provides dynamic data-level security controls and fine-grained data access governance for Oracle by serving as a SQL*Net proxy, allowing all calls from an Oracle Client to an Oracle 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 Oracle. DAE for Oracle 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 SQL*Net operates.

DAE for Oracle 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 Oracle enables employees and external partners to share critical information and collaborate in business processes to improve workforce productivity and business agility.

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

THE BENEFITS

DAE for Oracle 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 the data being accessed, the context of the request, and user identity. DAE dynamically applies the relevant policies, factoring in changes in the attributes of data or the 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, only 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.
Record-level Data Segregation and Filtering	DAE ensures that users can only view records or other data to which they have been granted access. Authorization can be determined based on the industry, location, department, position, project assignment, or any other attribute of the user, which can then be compared against other attributes of an entity or record such as sensitivity level, type of transaction, etc. For example, you can filter data in charts and reports to quickly identify inventory shortages in Thailand.
Granular enforcement of 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 SQL*Net proxy, allowing all applications that rely on SQL*Net to use DAE without any custom code required.

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®