NEXTLABS®

DATASHEET

Data Access Enforcer

Data Access Enforcer for SAP ERP Enterprise Edition

THE SITUATION

Organizations need to protect sensitive data, not only when it is being used by expected applications, but also from any unauthorized use when it is accessed in unexpected ways. To ensure this protection, many regulatory bodies require that sensitive data is encrypted not only when it is in use or in motion but also where it is stored, or at rest. Regulations like GDPR require this to protect against unauthorized direct access of sensitive data. This does not eliminate the need to share information quickly and easily across organizations and geographies, including roadmaps, product designs, inventory forecasts, etc., both internally and externally (e.g., with contractors, suppliers, and partners).

A challenge for organizations is in striking a balance between giving stakeholders access to sensitive data on one hand and the need to protect business critical data while adhering to applicable compliance requirements on the other. Organizations need data protection solutions that protect data with masking at rest, masking the data in a way that the data does not appear masked, and allowing that masking to be reversible for users that are authorized to access it. Information needs to be available to users on a need-to-know basis, following the principle of least privileged access, providing no more access or entitlements to protected data than the minimum that is needed.

THE SOLUTION

NextLabs Data Access Enforcer for SAP (DAE for SAP) Enterprise Edition provides organizations the ability to apply masking to data fields with sensitive data at rest, with masking that is both reversible and non-obtrusive, so that both applications and users seeing the masked data do not have to modify their business processes. This is in addition to all the dynamic data-level security controls and fine-grained data access governance for SAP applications included in DAE for SAP Standard Edition. DAE for SAP Enterprise Edition's Format Preserving Encryption (FPE) masking can be applied to data both at rest in the database, as well as in motion at the time of the data access request.

With NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policies and centralized policy management to improve their security and compliance posture for SAP, implementing the principle of least privileged access by granting access and entitlements on a need-to-know basis. DAE for SAP Enterprise Edition enforces data-level security controls, allowing organizations to combine field-level data masking with FPE and record level data segregation while monitoring data access activity from within the data access layer of the SAP S/4 HANA and SAP ECC.

Both DAE for SAP Standard and Enterprise Editions complement SAP Dynamic Authorization Management (SAP DAM), which operates at the application layers of the SAP S/4 HANA and SAP ECC. DAE is UI, API, microservice, batch job, report, Transaction, and Fiori app independent – and will support any UI with a single set of policies within a single solution.

DAE for SAP Enterprise Edition prevents unauthorized direct access to sensitive SAP data through fine-grained data-level security controls, protecting data both in motion and at rest and addressing compliance requirements at the same time. DAE for SAP Enterprise Edition enables employees and external partners to share critical information and collaborate in business processes to improve workforce productivity and business agility. With DAE for SAP Enterprise Edition, organizations can mask sensitive data at rest in a way that is not obvious to users who see the masked data and can reverse that masking for users that are authorized to access the data.

THE BENEFITS

DAE for SAP Enterprise Edition is a policy-driven data-centric security solution that uses dynamic authorization to enforce data-level entitlement and data security controls natively to protect SAP data in real-time. Benefits include the following:

Protect Sensitive Data

Leverage an SAP data-model aware and transactional data access level enforcement system to control data manipulation operations and protect data across all SAP applications. Mask sensitive data at rest, using FPE so that it does not appear obviously masked to users who are not authorized to access it, and dynamically unmask that data for users who do have the authorization to access and use the data. DAE for SAP Enterprise Edition's policies control authorized operations on business-critical data and mask and filter sensitive data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

Ensure and Streamline Compliance

Create information barriers to segregate regulated data or confidential projects to avoid data spills or contamination. Manage, educate, enforce, and audit access policies to sensitive corporate data to ensure compliance with regulations such as GDPR, ITAR/EAR, and SOX. Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. Provides comprehensive visibility about who is accessing what data and when, identifies anomalies before they become major breaches, and monitors and tracks events for audit, oversight, and investigation.

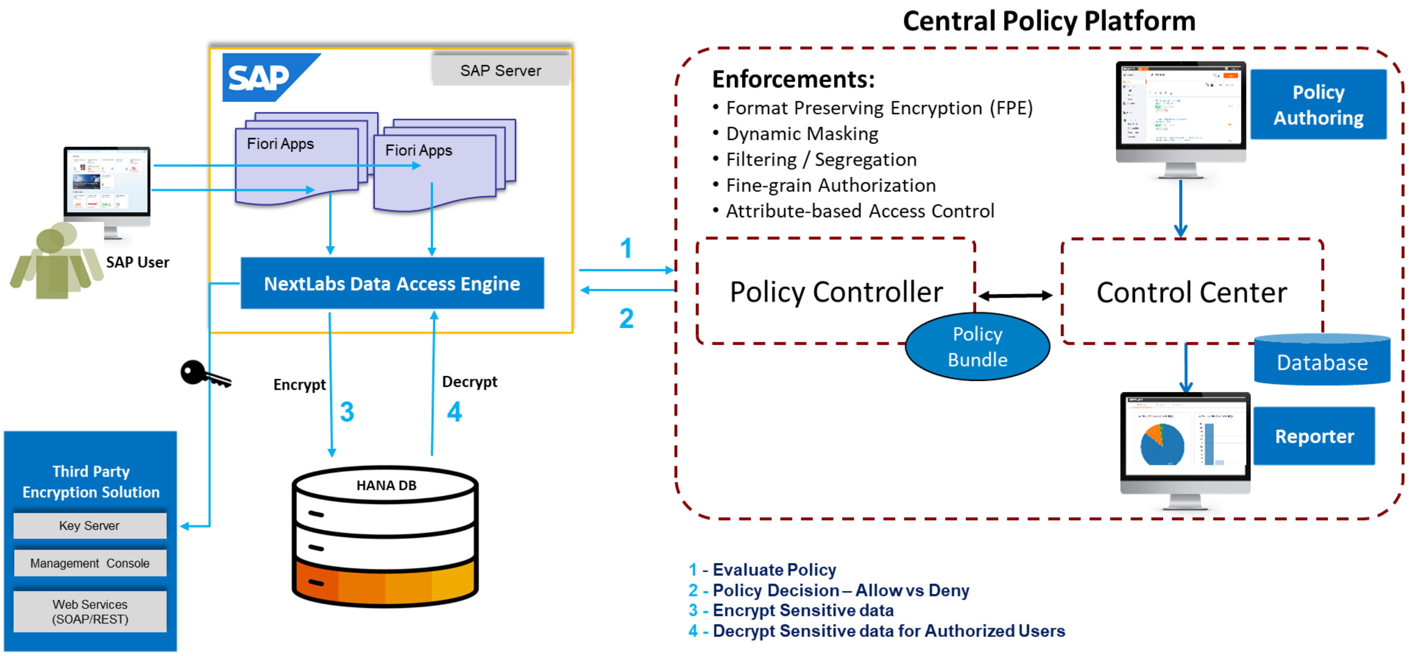
Improve Business Agility

Works natively with SAP and manages authorization logic through an externalized, standards-based policy framework. This slashes application development time and automates change management processes, enhancing business agility.

Reduce security and compliance management costs

Eliminate the need to implement and maintain costly customizations to meet security, compliance, and governance requirements. Attribute-driven dynamic authorization eliminates the need to maintain multiple SAP instances or manage individual authorization or user groups. DAE's Bulk Obfuscation Tool (BOT) allows organizations to simply and easily apply FPE masking to existing data in multiple fields and tables within a database, ensuring that all data at rest is obfuscated consistently and efficiently pre and post implementation of DAE.

DAE for SAP Enterprise Edition High Level Architecture



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 Dynamic 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, dynamically masking the value of the field for which users are not authorized. It uses policy-driven approach to mask the data in the unauthorized fields based on attributes at the time of data access. These centrally managed 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 or in motion 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 SAP ERP Enterprise Edition includes a built-in FPE library or can integrate with 3rd party encryption tools, such as Micro Focus Voltage. DAE' 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 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	No custom code required for SAP and third-party applications that use SAP HANA.

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 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.