NEXTLABS®

DATASHEET

Data Access Enforcer

Data Access Enforcer for SAP Test Data

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 such protection, many regulations, such as GDPR and Export Control, require encryption of sensitive data not only when it is in use or in motion but also when stored or at rest. Yet, this requirement 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 lies in balancing between the need to give stakeholders access to sensitive data and the need to protect business-critical data while adhering to compliance requirements . Organizations need data protection solutions that mask data at rest, masking the data in a way so that it appears unmasked, and reversing the masking for authorized users. 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 needed. It is common for organizations to keep non-production environments less restrictive but have production data used in those environments, which makes data protection in non-production environment critical. A combination of scrambling and subsetting functionality can thus be used to prevent unauthorized access to data in non-production environments.

THE SOLUTION

NextLabs Data Access Enforcer for SAP Test Data (DAE for SAP Test Data) provides organizations the ability to apply scrambling to data fields with sensitive data at rest that is both reversible and non-obtrusive, so that both applications and users seeing the scrambled data do not have to modify their technical integrations or business processes. This obfuscation of data at rest is in addition to the dynamic data-level security controls and fine-grained data access governance for SAP applications in the DAE for SAP product line. DAE for SAP Test Data's Format Preserving Encryption (FPE) masking can be applied to data at rest in the database so that when data is extracted from production databases, it is scrambled and the original data is not exposed to unauthorized users or systems.

With NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policies and centralized policy management to limit access to original values in test data sets. This is done by implementing the principle of least privileged access, granting access and entitlements on a need-to-know basis. DAE for SAP Test Data enforces data-level security controls, allowing organizations to scramble data at rest with FPE and use subsetting to prevent unauthorized access to data while allowing organizations to use test data sets in their non-production environments.

DAE for SAP Test Data complements the DAE for SAP product line, ensuring the protection of data is consistently enforced in both production and non-product environments. This is because DAE operates at the data access layer of SAP systems and 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 Test Data prevents unauthorized direct access to sensitive SAP data through fine-grained data-level security controls, protecting data both in motion between production and non-production environments and at rest within the database. DAE for SAP Test Data enables employees and external partners to use scrambled data in non-production systems that simulates real data, and also allows for the authorized unscrambling of that data when needed by authorized systems or individuals for testing purposes.

THE BENEFITS

DAE for SAP Test Data is a policy-driven, data-centric security solution that uses dynamic authorization to enforce data-level entitlement and security controls natively. DAE restricts access to controlled data while unscrambling it in real-time for authorized users who need access to the original data values. Benefits include the following:

Protect Sensitive Data

Leverage an SAP data-model aware and data access level enforcement system to protect test data across all SAP applications and across both production and non-production environments. Scramble sensitive data at rest using FPE so that it can still be used in non-production environments by systems and users who are not authorized to access the original data, and dynamically unmask that data selectively for authorized users and systems to use for testing. DAE for SAP Test Data's policies combine scrambling and subsetting of 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 prevent unauthorized access to regulated data or confidential projects and avoid data spills or contamination when exporting data from production environments to use for testing. 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. Provide comprehensive visibility around who is accessing what data and when, identify anomalies before they become major breaches, monitor and track events for audit, oversight, and investigation.

Maintain Referential Integrity

DAE can apply format preserving encryption (FPE) to data such that keys and identifiers can still be used and referential integrity is maintained even when data has been scrambled. This allows systems that rely on such references to be fully tested in non-production environments without requiring access to restricted data.

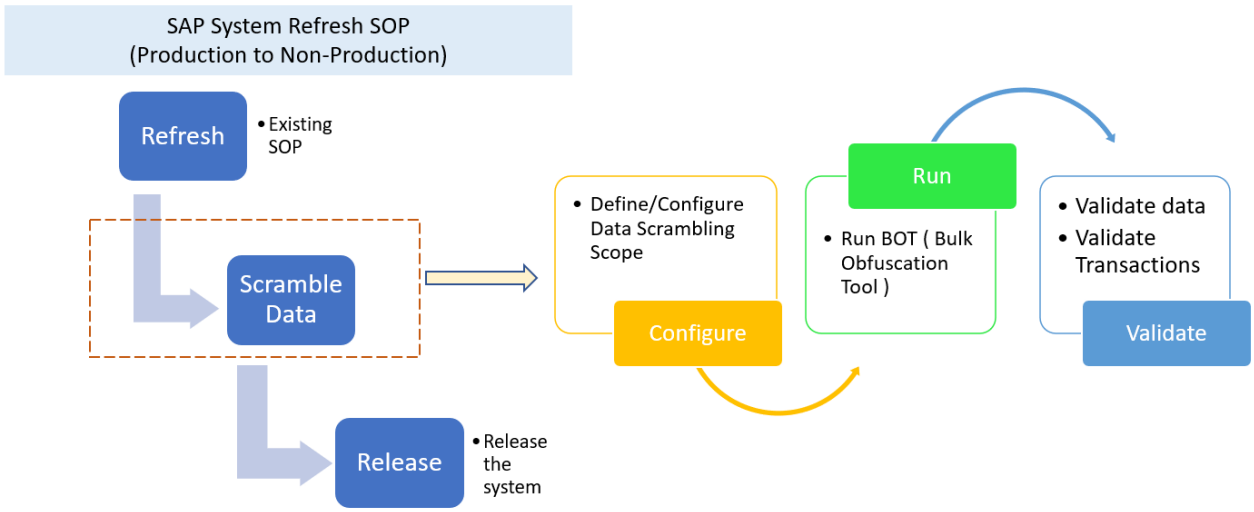
Improve Business Agility

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 of test data sets 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.

Data Scrambling using NextLabs



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	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 and Scrambling	Elements in the DB data store can be masked or scrambled at rest, ensuring that the scrambled data in test data sets preserves the length and format of the original data, which is important for effective testing and maintaining application dependencies. Scrambling can be reversed to allow authorized users and systems to use the original data when necessary for testing. DAE for SAP Test Data includes a built-in FPE library or can integrate with 3rd party encryption tools, such as Micro Focus Voltage. 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 Subsetting and Data Segregation and Filtering	DAE ensures that users can only view records or data they are authorized to access and that sensitive records are excluded when test data is exported from a production database. 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, when exporting customer data for use in testing you can exclude records of customers who reside in areas where regulations prevent such use of their data.
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.