NEXTLABS®

White Paper

Protect ERP Data and Improve Compliance with Dynamic Authorization and Zero Trust Principles

Prevent Wrongful Disclosure of Data Across Your Business Network

Businesses that support collaboration beyond their boundaries benefit greatly from improved innovation and productivity. But how do you prevent wrongful disclosure while enabling your employees and partners to share and collaborate? How can you work closely with partners and an extended supplier network to design and manufacture best-in-class products?

A successful collaboration depends on the ability to share information quickly and easily internally and with third-party companies, working across organizational and geographical boundaries. However, it is vital to balance the need to provide ready access to enterprise data while protecting privacy data, valuable intellectual property, and sensitive corporate information. In addition, you must meet a number of industry-, country-, or region-specific compliance requirements.

Data Access Enforcer (DAE) for SAP by NextLabs helps you achieve this balance, maximizing your existing investment in SAP applications. With DAE for SAP, you can provide real-time, secure, attribute-based segregation and masking for enterprise data within your SAP business applications. Sophisticated dynamic authorization logic helps ensure that you automatically adhere to data security policies, and advanced auditing functionality allows you to monitor and document regulatory compliance.

Enforce Need-to-Know Policies for Enterprise Data Without Compromising Productivity

Collaboration is key for businesses that want to lead the way in innovation. But if employees and business partners must wait too long to access the information they need; productivity may suffer, and your initiatives may stall.

DAE for SAP incorporates an attribute-based access control (ABAC) model that enables dynamic criteria and preventive policies to be applied at the data access layer before granting access to enterprise data.

Additionally, DAE for SAP features simple policies that can be administered by business owners and rapidly applied to all connected systems. You can roll out new data protection policies instantly across your entire user base. This way, you can react rapidly to take advantage of business opportunities even when they involve a new set of compliance requirements.

Enable Data Protection at a Granular Level – with Automation

DAE for SAP uses ABAC functionality to segregate and obfuscate enterprise data in SAP applications. This means that the software uses contextual information in real time from different sources to determine the entitlements of each user. These policies are applied at the data access layer in such a way that is application independent, preventing the data a user is not authorized to access from making it into the SAP application, so the user does not even see that presence of the data they are not authorized to access.

DAE for SAP uses attribute-based access control (ABAC) policies to determine a user's access and entitlements to data. These policies are defined in terms of attributes of the user (e.g. title, business unit, project membership, citizenship, or clearance), the data (e.g. the value, data type, or classification), and the environmental context (e.g. IP address, time of day, geographical location) and are dynamically evaluated at the time of the access request. The policies enforce not only the user's access to the data, but also their entitlements (e.g. View, Update, Create, Delete).

To meet the requirements of your policies for enterprise data protection, DAE for SAP also enables you to set up specific actions each time a data access request is evaluated. For example, you can arrange for a message to be displayed on the user's screen, or for a message to be sent to inform a manager that the user has requested access to a particular data object. All access activities are logged and aggregated centrally to streamline the reporting process, which provides deep insight into who is accessing what data and when.

Cut Complexity in Data Protection

With DAE for SAP, you can streamline processes across your organization. You can automatically incorporate business rules and policies that will continuously govern access to your enterprise data based on the real-time state of your users. This saves time and frees up IT personnel to focus on other activities.

By establishing a centralized, integrated data protection solution, you can apply data segregation and masking rules as well as system-level authorization policies instantly from a single, common console. A single policy can now apply to all connected applications. This helps ensure consistent enterprise-wide management and enforcement of policies. It also helps accelerate the rollout of changes to data privacy and obfuscation policies.

In addition, DAE for SAP offers intuitive graphical interfaces for code-free administration of data protection policies. These enable even nontechnical users to manage and track policies throughout their lifecycle.

Fulfill Your Compliance Obligations Effectively

DAE for SAP helps you meet the data privacy requirements of tough enterprise data security and nondisclosure legislation such as export controls and the General Data Protection Regulation (GDPR).

The application enables you to establish robust data-segregation rules that comply with regulatory mandates. For instance, with the application, you can define data segregation and masking policies for all sources of personal data that GDPR aims to protect. DAE for SAP both protects that personal data and makes it easier to report accurately on the status of data objects. Advanced auditing tools enable you to track and report on access of sensitive enterprise data within SAP business applications. Run an audit on how critical data is used providing auditors with evidence of proper entitlements and your ability to audit, as well as proof of controls over your regulated information.

By logging all access to enterprise data in SAP applications through a single, centralized solution, you improve the efficiency of your reporting processes. This not only reduces risk of noncompliance but also helps you cut costs associated with lengthy audit investigations. See the figure on the next page for more on use cases.

Figure: Business Use Cases of DAE for SAP

Modernization	• Centralize and automate data protection policies for both legacy and new applications (such as SAP S/4HANA) • Adopt Zero Trust Architecture to modernize IT for better security, visibility, and control
SoD and Compliance	• Enforce segregation of duties (SoD) and segregation of data to help avoid violations • Comply with HIPAA, the California Consumer Privacy Act, General Data Protection Regulation, Sarbanes-Oxley Act, International Traffic in Arms, export policies, FDA regulations, and others
ERP Consolidation	• Protect critical data while consolidating ERPs into a single global instance
Mergers and Acquisitions	• Keep sensitive data safe while integrating new businesses • Segregate data of divesting businesses
Cybersecurity	• Reduce cybersecurity risks (create a cybersecurity framework compliant with the National Institute of Standards and Technology)
Trade Secrets	• Make sure only the right people have access to the right data by implementing need-to-know policies.
Automation	• Cut costs by automating business processes and internal controls

Extensive Support of SAP Applications

DAE for SAP supports SAP ECC, SAP S/4HANA®, SAP BW, SAP BW/4HANA, and SAP HANA. DAE is UI, API, microservice, batch job, ad-hoc query, report, transaction, and Fiori app independent and will support any UI, debug, and table content access with a single set of policies.

Make Sure the Right People Get the Right Data When They Need It

With DAE for SAP, you can automate the process of defining and updating data access policies. As a result, you can provide both your employees and your business partners with access to critical enterprise data while still enforcing need-to-know policies and preventing wrongful disclosure. This streamlines collaboration and fosters co-innovation across your business.

Intuitive, centralized control tools enable you to establish authorization rules across your business network, improving the consistency of these processes. In addition, the software helps you reduce the time it takes to implement new data protection policies or update existing ones. This dramatically reduces administration costs and frees up IT resources.

Sophisticated attribute-based authorization processing supports compliance with even the most complex data segregation and obfuscation policies. Combined with real-time preventive SoD and data-centric security controls, the software helps prevent sensitive enterprise data from falling into the wrong hands and minimizes the risk of noncompliance penalties such as fines. You can monitor information usage to learn who is accessing and distributing governed data. Meanwhile, advanced reporting tools allow you to report on the application of data protection policies efficiently, accurately, and quickly.

Summary

With the DAE for SAP by NextLabs, you can prevent wrongful disclosure across your business network, whenever and however that data is accessed. The software enables employees and external partners to share critical information, encouraging collaboration and co-innovation and boosting productivity. You can streamline data protection processes and comply with

Objectives

- Prevent wrongful disclosure of critical enterprise data
- Enable the global sharing of information necessary for designing dynamic products
- Safeguard vital corporate intellectual property while meeting regulatory requirements

Solution

- Granular, attribute-based data segregation and obfuscation enforced at the data access level
- Centralized data protection policy management
- Virtual data segregation with view and field-level data security controls
- Anonymization of data with Format Preserving Encryption (FPE) to protect critical data at rest
- Alerts and reports on access to critical data in SAP applications

Benefits

- Enable secure collaboration across the business
- Enhance compliance and avoid risk by enforcing need-to-know and sharing policies
- Increase efficiency and savings by automating data protection
- Apply consistent data segregation and obfuscation policies across SAP applications