opentext™ | Cybersecurity NEXTLABS®

Solution Flyer

Protecting Data in SAP with Voltage SecureData and NextLabs

A proven data-centric approach to protecting sensitive data in SAP

Voltage SecureData at a Glance

Voltage SecureData by OpenText offers an end-to-end data-centric approach to enterprise data protection. It is the only comprehensive data protection platform that enables you to protect data over its entire lifecycle—from the point at which it's captured, throughout its movement across your extended enterprise, all without exposing live information to high-risk, high-threat environments.

The Challenge: Schrems II and the Need for Data-Centric Protection

Schrems II and the strong move to hyperscalers by SAP customers have made the topic of protecting data at rest, in motion and in use even more critical for SAP customers. Data should be protected to safeguard it from unauthorized access in case of a data breach or theft, but also to protect against Database Administrator (DBA) risks. A data-centric approach to protection ensures that even if an attacker or unauthorized user gains direct access to data even when they extract it from the database (Schrems II). Attackers will not be able to read the protected data. This helps to safeguard sensitive information such as personally identifiable information (PII), financial data, and intellectual property.

Data-centric protection is a best practice for data security and is often required by regulations and compliance standards such as the GDPR, HIPAA, Export Control regulations, Good Practices (GxP) and PCI DSS. Depending on user privileges, data can be accessed in the clear, dynamically filtered, dynamically masked, encrypted or tokenized to support the broadest range of use cases.

How It Works: Voltage SecureData for SAP

Voltage SecureData for SAP is a combination of the best technologies in the market, from OpenText Voltage and NextLabs, providing encryption of data in the database, in transit and even while in use coupled with dynamic access controls.

Through Voltage SecureData, data-level security controls such as field-level data masking, format-preserving encryption (FPE) and tokenization are provided for both SAP S/4 HANA and SAP ECC.

With NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policy and centralized policy management to improve their security and compliance posture for SAP.

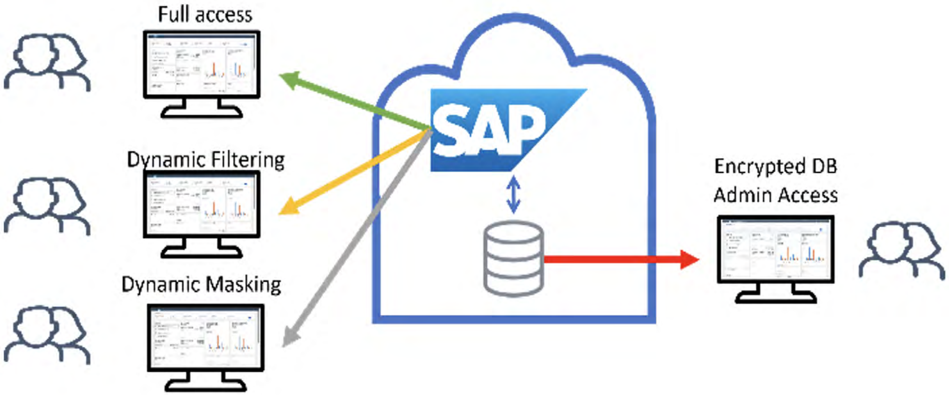


Figure 1.

OpenText Voltage Format-Preserving Protection Support for SAP

Voltage SecureData's privacy-enabling protection techniques apply strong protection (whether it be encryption, data masking, tokenization, or hashing) to specific fields of data at rest, in motion and in use.

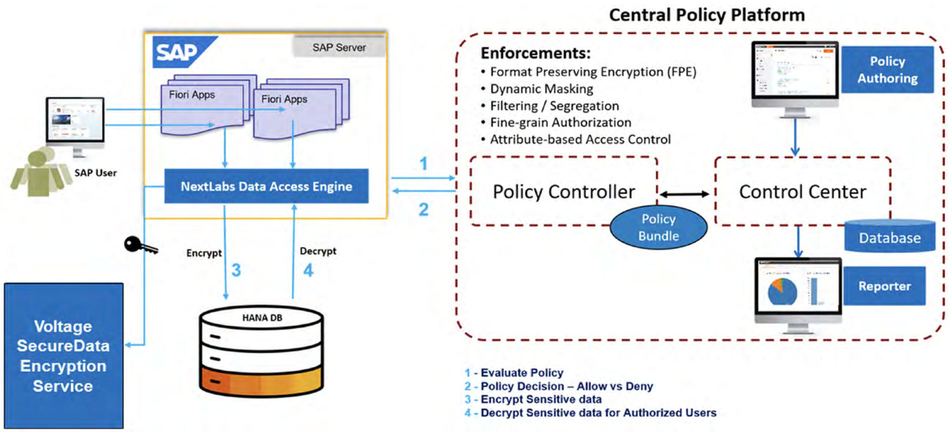
Format-preserving protection ensures that applications can process the protected content—i.e., a protected email address still looks like a valid email address. The data is unprotected only for authorized users at the time of a valid data access request.
Key Features of the combined solution are:

- Policy-driven capability to perform field and column level format-preserving encryption, tokenization or hashing together with field-level data masking and record filtering based on dynamic attributes

Enabling Data Privacy Compliance

Voltage SecureData protects any sensitive data, using an array of format-preserving data protection techniques to address compliance to privacy, payments standards and regulations, and data security needs.

Connect with Us
www.CyberRes.com



1 - Evaluate Policy
2 - Policy Decision – Allow vs Deny
3 - Encrypt Sensitive data
4 - Decrypt Sensitive data for Authorized Users

Figure 2. High-Level Architecture

- Supports any data format including but not limited to Names, Addresses, Email-addresses and Credit Card Numbers, including Numeric, Alphanumeric and Date formats as well as the ability to preserve aspects of data for partial protection of data (i.e., trailing 4 digits in credit card and leading 4, etc.)
- Eliminates changes to database or application schemas—data "fits" in existing fields
- Maintains data referential integrity for processes, applications, and services
- Highest availability and scalability with stateless software and HSM-based key derivation and management such as seamless key rotation, Bring Your Own Key (BYOK), etc.

Voltage SecureData for SAP Benefits

The joint OpenText Voltage / NextLabs solution uses a variety of options (encryption, tokenization, hashing and masking) to protect sensitive data at rest, in motion, and in use. Voltage SecureData "de-identifies" data with market-leading performance and scale, rendering data useless to attackers while maintaining its usability, usefulness, and referential integrity for data processes, applications, and services. Voltage SecureData neutralizes the risk of data breaches by making protected data worthless to an attacker, whether it is in production, analytic systems, or test/development systems such as training and quality assurance.

Voltage SecureData with NextLabs Data Access Engine (DAE) for SAP integration allows customers to use an existing instance of Voltage SecureData to encrypt and decrypt the data for SAP. Customers can use any of the formats to be protected by Voltage SecureData when defining policies in NextLabs CloudAz.

By providing an out-of-the-box integration to Voltage SecureData, NextLabs DAE for SAP allows customers to utilize the format-preserving protection capabilities of Voltage SecureData to protect their SAP data without the development and maintenance of their own custom code. Configuration of DAE for SAP to use Voltage SecureData is as simple as updating the DAE properties file to specify that Voltage SecureData should be used, along with the location and connection information for the Voltage SecureData server. No custom coding is required.

Key benefits include seamless integration and smooth operation, applying proven data protection to meet current and future regulatory requirements.

Learn more at
www.microfocus.com/en-us/cyberres/data-privacy-protection/securedata-enterprise

www.nextlabs.com/products/data-access-security-with-dynamic-data-masking/

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000111-001 | O | 08/23 | © 2023 Open Text