opentext™ | Cybersecurity

Solution Flyer

Voltage Data Privacy Manager

Secure and compliant test data management

Voltage Data Privacy Manager at a Glance

Voltage Data Privacy Manager takes the risk out of using production data in non-production test data environments with these vital functions:

- Discovering private data in databases
- Enabling data privacy and protection in non-production environments
- Anonymizing data for secure use whether for analytics, test, or other use cases
- Shielding real data sources with a protected Test Data Repository containing realistic "fake" data
- Ensuring that the real sensitive data is secure

Data Privacy Laws Are Changing the Landscape of Test Data Management

Many companies have been using real production data to make sure that application testing is relevant and captures the variety of use cases they may have. Production data inevitably includes sensitive personal data. Data privacy laws (such as GDPR, CCPA, and KVKK) now prohibit and obligate companies to protect citizen data even when consumed internally. Some organizations sub-contract their testing, Quality Assurance (QA), and training processes to third parties located in different countries, exposing citizen data to non-authorized users. Such practices are automatically non-compliant with data privacy laws.

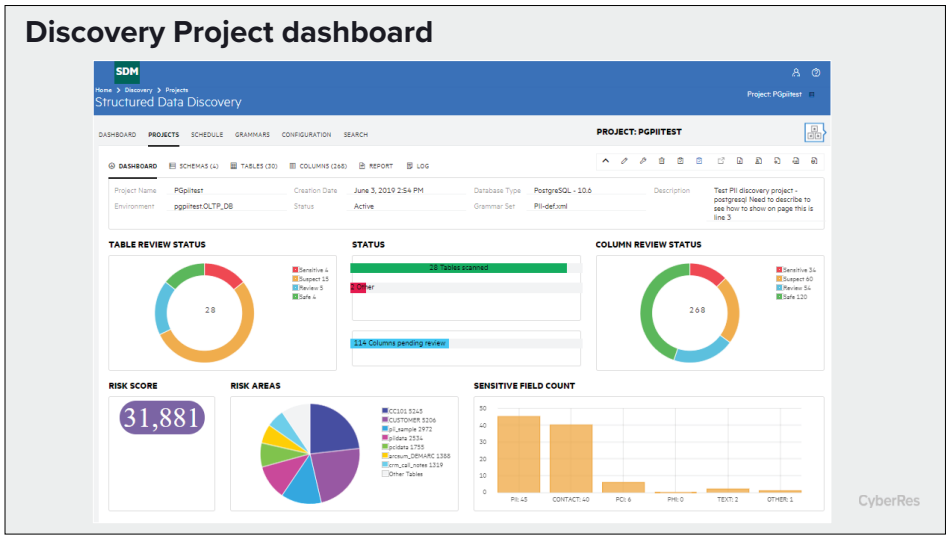
To enable data privacy, businesses need to ensure that every data element is identified, classified, and protected according to the population of users and policies. Considerations must be made for data across all environments. Whether a customer's personal data is in a production database, an archive, or a test database, a data breach will still affect that person, and trigger non-compliance fines and penalties for the business. Additional critical data privacy management capabilities include being able to prove data is not reversible, and responding to privacy auditors' requests to verify that test and analytics data values are truly anonymized and cannot be reverted to the original values.

Voltage Data Privacy Manager by OpenText™ provides a comprehensive solution to address the privacy governance needs of

enterprises with sensitive structured data. It provides a single solution for sensitive data discovery, extraction, and anonymization, to deliver test data that closely matches production data and is compliant with data privacy regulations. As it offers a range of data protection techniques, Voltage Data Privacy Manager also enables customers to manage and protect sensitive structured data throughout its lifecycle, from discovery and classification to protection and disposition.

Discover Private Data in Databases

To help ensure data privacy, businesses must first understand their data and map their sensitive data sources and data flows. Then protection policies for testing, QA, and development can be applied. Voltage Data Privacy Manager finds sensitive structured data in active and inactive systems across the enterprise. Often there is a gap between what a data element was designed to contain and how end-users are populating it to serve their purpose. Voltage Data Privacy Manager discovers the real meaning of the data contained in any data element and creates an inventory of what needs to be protected and how for any data source.



Enable Data Privacy in Non-Production Environments

Generating non-meaningful test data for performance testing is not a difficult exercise, but generating meaningful data that looks and behaves like real production data for functional testing is the challenge. Meaningful data contains all the characteristics of production data, such as format, context, and referential integrity, but is anonymized for data privacy compliance.

While developing an application, developers need to make sure they are testing it under conditions that closely simulate a production environment. Most tests rely on sample data for testing. If the data is manually entered into a test environment, it cannot match the volume and variety of data that the application normally would accumulate in production. Behavior may differ because data inserted into the test database will not match real-world usage, possibly leaving significant bugs. Dev/test managers, application owners, and others know that simulated data fails to effectively support development, and manual scripting cannot keep up with the demand for fast timelines between application development and production.

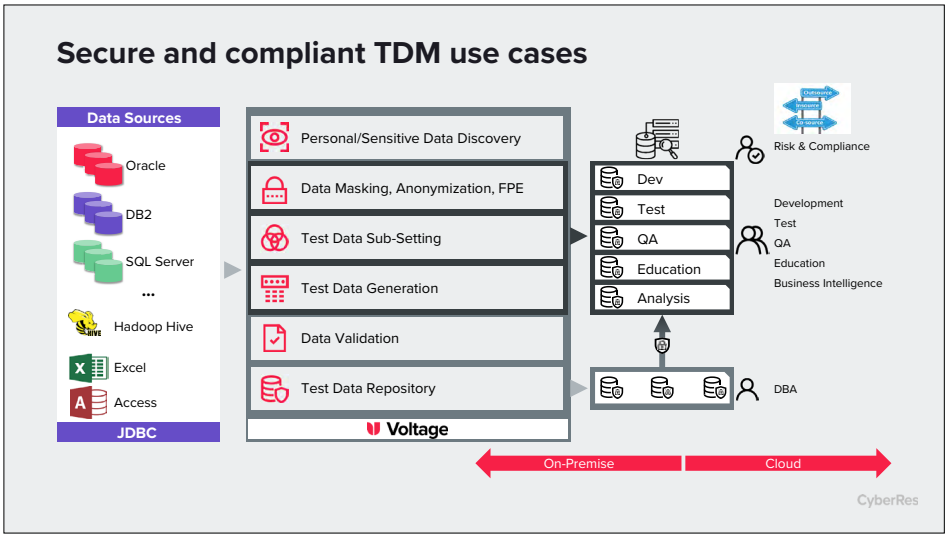
Building a test database with meaningful, protected test data allows the application owner to see and assess how the application will perform once it released. Without meaningful test data in the test environment, it is impossible to predict the way the application will behave after the release.

Organizations testing non-production data want to see data that looks real to understand how real data would perform in their application. For example:

- For a first name, see a fake real first name that corresponds to the sex of the person
- For a last name, see a fake real last name
- For a ZIP code, see a fake real ZIP code existing in the state of the address
- For a state, see a fake real state code that exists in the country of the address
- For a credit card, see a fake credit card number that resembles a real one
- For a date of birth, see a plausible date of birth
- For an amount, see a plausible amount for the context
- For any data type, see a fake meaningful value

Anonymize the Data for Secure Use Whether for Analytics, Test, or Other Use Cases

Because the evolving privacy landscape now makes it impossible to use real data for testing, it is essential to have a tool that can generate protected and anonymized data that appears real. Voltage Data Privacy Manager anonymizes personal and sensitive data such as credit card information, U.S. Social Security and other national ID numbers, names, addresses, and phone numbers—virtually any data types and language.



Shield Real Data Sources with a Protected Test Data Repository Containing Realistic Fake Data

Voltage Data Privacy Manager provides a Test Data Repository that shields real production data from any access by non-authorized users and minimizes workload on real data sources from test extractions.

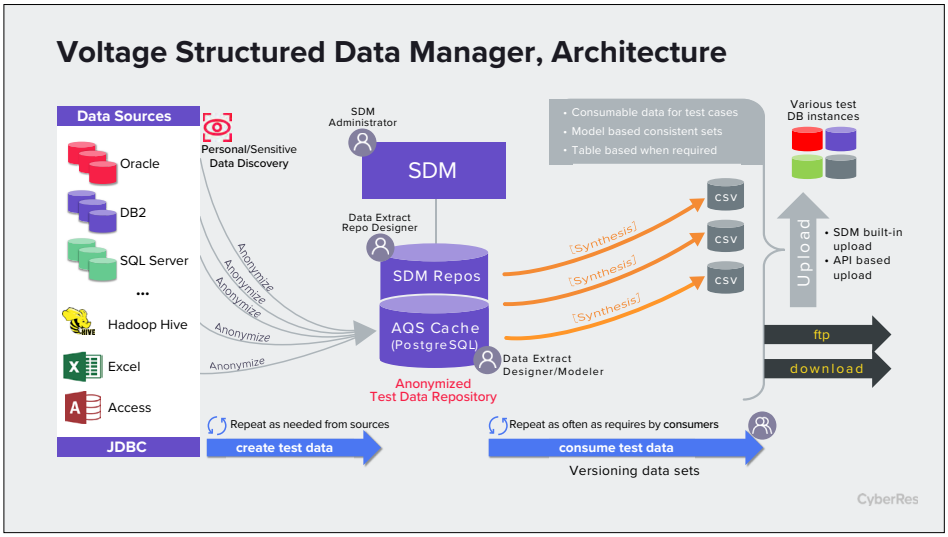
The Test Data Repository is secured and contains only generated data (meaningful data):

- Randomly generated from dictionaries (file- or SQL-based)
- Randomly shuffled from the data set (SQL-based)
- Randomly selected with preserved context; generate feminine name if sex is female, masculine otherwise; generate meaningful address depending on ZIP code; etc.
- Algorithmically generated via random anonymization or user-defined transformation
- Consistent data: for any given input value, get the same randomly created value, providing consistency across disparate data stores

Ensuring That the Real Sensitive Data Is Secure

There are numerous approaches to keeping sensitive data protected from exposure. Transforming data at use so the end-user never sees real data is appealing, but is not secure because any access outside of the application will see real data. Recent data breach cases have clearly shown that the best method is to persistently protect data by default—at rest, in motion, and in use. This means protecting the data as soon as possible—preferably at entry—and then leaving it protected except for the few cases where the real data is truly required. Multiple approaches are available with Voltage Data Privacy Manager including extracting data for archiving and test data management use cases.

Voltage Data Privacy Manager can generate realistic fake contextual data to be used by



testers or learners in databases where they do not have the privilege to see the real data. Multiple mechanisms are offered to enable proper protection of the data, including Format-Preserving Encryption (FPE), Format-Preserving Hash (FPH), Random Generation of Meaningful Values (RGMV), Random Generation of Meaningful Unique Values (RGMUV), Random Mapped Generation of Meaningful Values (RMGMV), and Random Mapped Generation of Meaningful Unique Values (RMGMUV), which mask sensitive data contained in text, comments and notes, or any custom transformation.

Produce Private Data

Voltage DPM offers a self-service portal (web-interface) to guide users on how they can produce private data. It also provides command line and APIs to automate the production of private data when integration with other tools is required (e.g., test data automation processes).

Voltage Data Privacy Manager

Data Privacy Manager merges leading Voltage Products by OpenText™ products: Structured Data Manager and Voltage SecureData by OpenText™.

Voltage Structured Data Manager (SDM) by OpenText™ enables complete management of structured data across its lifecycle. Voltage SDM can discover sensitive data in on-premises, cloud, or hybrid systems and classify in-scope data for disposition. Voltage SDM enables policy-based disposition of data, defining archival, protection, deletion, or any other disposition based on company policy. Completing the process, Voltage Structured Data Manager records all actions taken and can produce detailed reports for compliance audits. Voltage SDM performs all this through a user-friendly interface that allows structured data to be managed throughout the enterprise from a single pane of glass.

Voltage SecureData provides an end-to-end data-centric approach for enterprise data protection. By leveraging Voltage Format-Preserving Encryption (FPE), Format-Preserving Hash (FPH), Secure Stateless Tokenization, and Stateless Key Management, SecureData protects sensitive structured data over its entire lifecycle—from the point at which it's captured and throughout its movement across the extended enterprise, without gaps in security. Voltage SDM de-identifies data, rendering it useless to attackers, while maintaining its

usability and referential integrity for data processes, applications, and services. Voltage SecureData enables the adoption of a continuous data protection model wherever data flows, in analytic platforms and applications in hybrid multi-cloud environments and native cloud-services.

Whether the enterprise is working to comply with legislation such as GDPR, CCPA, and KVKK, protect big data projects, adopt hybrid IT, or protect legacy systems, Voltage Data Privacy Manager provides for management, protection, and privacy of structured data throughout its lifecycle. Enterprises can comprehensively discover, classify, protect, manage, and audit sensitive data across the organization: in the cloud, legacy systems, test environments, and production or storage servers.

Key Benefits

- Support compliance with data privacy mandates and regulations
- Improve the security of test and analytics environments
- Automate test data management
- Reduce complexity with simplified test data generation
- Reduce the risk of data misuse or loss
- Protect data from unauthorized access

TDM Deployment

- Windows or Linux
- Physical or virtual machine
- Cloud or on-premise

Data Sources

- Oracle
- DB2 LUW
- DB2 z/OS
- SQL Server
- PostgreSQL
- MySQL
- Sybase
- Informix
- Hadoop-Hive
- MongoDB
- Cassandra
- Any JDBC compliant source

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

761-000036-005 | O | 10/23 | © 2023 Open Text