Solutions Flyer
Security

MICRO FOCUS

Securing Sensitive Data in Teradata

A unique, proven data-centric approach to the protection of sensitive data in the Teradata ecosystem.

Voltage SecureData at a Glance

Voltage is a leading expert in data-centric encryption and tokenization technologies, providing complete protection for personal identity information, health information, primary account numbers, and other kinds of sensitive data.

The Challenge: Securing Sensitive Data for Use in Analytics

Decision makers must have ready access to all relevant data. Making decisions without the right data means the difference between a successful business venture and a failed one. But it's not always easy to get access to the data you need, especially when data resides in multiple, disparate databases, data lakes, and data warehouses. With ever-increasing competitive and cost pressures, enterprises are driving toward greater use of big data analytics to extract more value from corporate and customer information.

At the same time, concerns for effective enterprise data security and compliance with privacy regulations can often cause delays in adopting these valuable technologies. As with any deployment of enterprise data architecture, you face many security and regulatory compliance challenges. Especially when replicating data automatically across multiple nodes, handling multiple types of data, or enabling access to many different users with varying analytic needs and access roles. With data in constant motion and with rising threats to sensitive data from both inside and outside the enterprise, organizations need to be able to protect data end-to-end, from the moment of capture across the information lifecycle including testing and production.

An End-to-end Solution Is Needed

The Teradata analytics platform makes it easy to transform data into meaningful insights. The Teradata architecture is designed so you can analyze anything, deploy anywhere, and make smarter decisions based on relevant answers.

Voltage SecureData for Teradata protects sensitive structured data at the field level for persistent protection of data in use, in motion, and at rest across hybrid IT. With SecureData, privacy of sensitive information is preserved end-to-end across an enterprise's IT infrastructure—from the moment of capture through business analysis applications, and to the back-end data store. With format-preserving encryption (FPE), hash, and secure stateless tokenization (SST) from Voltage, protection is applied at the data level, preserving characteristics of the original data, including numbers, symbols, letters, and numeric relationships such as date and salary ranges. It also maintains referential integrity across distributed data sets so joined data tables continue to operate properly.

Voltage Stateless Key Management

Traditional key management for encryption effectively reduces the data protection posture of an organization due to the key vault and ongoing key management requirements which leave gaps in protection and increase opportunities for cyberattack. In contrast, Voltage Stateless Key Management raises the security posture of an organization through elimination of the key vault, key management staffing, and related costs. As a result Voltage Stateless Key Management differentiates Voltage Format-Preserving Encryption even over alternative types of data-centric protection, and significantly reduces Total Cost of Ownership (TCO) over any traditional or data-centric approach. Most global enterprises support SecureData with 0.1 of a Full-time Equivalent (FTE) employee. For those enterprises using an active/active architecture with dual data centers, Voltage Stateless Key Management enables High Availability and instant Disaster Recovery (DR).

Data Protection from the Source

Voltage SecureData is a certified technology partner with Teradata. SecureData encryption and tokenization can be applied at the source before ingestion into Teradata or invoked during an ETL transfer. Data may also be protected in source databases, mainframes, or other systems, as well as moved in its protected form directly into the Teradata ecosystem.

In Teradata, protected data can be used in its de-identified state for additional processing and analysis without further interaction with the Voltage SecureData system. Or the analytic programs can access clear text by utilizing the SecureData high-speed decryption and detokenization interfaces with the appropriate level of authentication and authorization.

If processed data needs to be exported to downstream analytics in the clear—such as into a data warehouse for traditional BI analysis—there are multiple options for re-identifying the data, either as it exits Teradata database, or as it enters other downstream processing systems. Customers can apply SecureData for Teradata in a number of ways. See Figure 1 on the following page for more details.

How It Works

Seven specific Voltage SecureData options protect sensitive data in Teradata as follows:

- Apply data protection at source applications
- Apply data protection during import into a landing zone (ETL process)
- Apply data protection during Teradata import processing or import into a Hadoop data lake (e.g., SQL, Sqoop, MapReduce, Hive, Apache NiFi, Storm/Kafka)
- Use de-identified data within Teradata
- Use and export re-identified data from Teradata or Hadoop (SQL, Hive, etc.)
- Export data and re-identify outside of Teradata (ETL process)
- Use storage-level encryption within Hadoop

Voltage SecureData and Teradata bring a unique, proven, data-centric approach to the protection of sensitive data in big data environments, which is essential to enabling secure analytics in Teradata whether on-premises or in the cloud.

Enabling Data Privacy Compliance

Voltage SecureData is a leader in format-preserving data encryption, pseudonymisation, tokenization, and anonymisation solutions for enterprise data privacy, regulatory compliance and protection of data analytics.

Benefits of SecureData for Teradata

- Securing TCore at scale anywhere, always
- Enabling data privacy compliance in analytics
- Assuring data protection portability in hybrid IT

About Voltage SecureData

Voltage SecureData is a leader in data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise and mobile environments with continuous protection.

Voltage SecureData brings a unique, proven data-centric approach to the protection of sensitive data in the Teradata Ecosystem and the ability to significantly reduce the scope of regulatory compliance audits. SecureData calls for de-identifying the data as close to its source as possible, transforming sensitive data elements into usable (yet still de-identified) equivalents that retain their format, behavior, and meaning.

Protected data can be used in subsequent applications, analytic engines, data transfers, and data stores, and securely re-identified only for those specific applications and users that require it.

Voltage SecureData Benefits

- The ability to protect data as close to its source as possible
- Support for encryption, tokenization, and data masking protection techniques
- Supports the encryption, pseudonymization, and anonymization guidance in the GDPR (General Data Protection Regulation) legislation for European Union, and beyond.

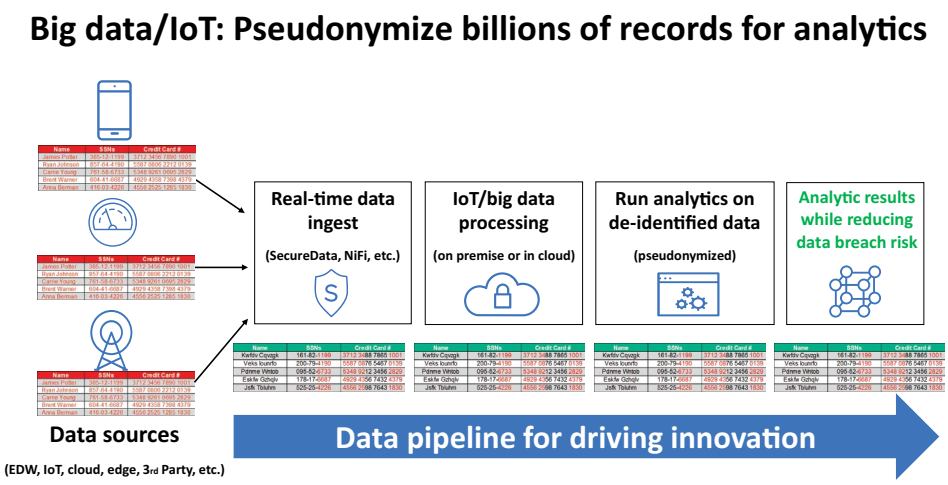

Figure 1. How it Works: Pseudonymize billions of records for analytic insights

Voltage SecureData for Teradata is a comprehensive data protection framework that secures data as it is captured, processed, and stored across a variety of devices, operating systems, databases, and applications.

Contact us at:
www.microfocus.com

Like what you read? Share it.

- Ability to encrypt data of any type, any language, any region with format-preserving encryption, unique in the industry
- Data usable for many applications in its de-identified state
- The ability to securely re-identity data when required—only by authorized users and applications
- The industry's first Federal Information Processing Standard (FIPS) 140-2 validation of FPE, and the world's first FIPS-validated AES-FF1 encryption configuration option to operate in strict FIPS mode.
- Enable significant reduction of scope and costs for regulatory audits such as PCI and HIPAA
- Protection techniques backed by security proofs and standards
- High performance, high scalability, and well matched with big data speeds
- Broad platform and application support—inside and outside Teradata ecosystem

Micro Focus Voltage Enables the World's Leading Brands to Neutralize Data Breach Impact for Data at Rest, in Motion and in Use by De-Identifying Sensitive Information

Micro Focus® Voltage data security solutions enable advanced format-preserving encryption, secure stateless tokenization, and stateless key management to protect enterprise applications, data processing infrastructure, hybrid IT/cloud, payment ecosystems, mission-critical systems, storage, and big data/IoT analytics platforms. Voltage data security solutions solve the industry's biggest challenge by simplifying data protection across complex legacy and modern IT, enabling organizations worldwide to comply with privacy mandates with confidence and trust, while driving digital transformation for value creation.

Learn more at
www.microfocus.com/securedata