MICRO FOCUS

Solution Flyer

Voltage SecureData
Voltage SecureData for Teradata

Securing Sensitive Data in the Teradata UDA

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

Voltage SecureData at a Glance

Voltage SecureData 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.

Product Snapshot

Voltage SecureData for Teradata UDA 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.

Solution Highlights

Voltage SecureData brings a unique, proven data-centric approach to the protection of sensitive data in the Teradata Ecosystem and the ability to reduce the scope of regulatory compliance audits significantly. SecureData calls for de-identifying the data as close to its source as possible, transforming sensitive data elements with usable, yet de-identified, equivalents that retain their format, behavior, and meaning. This protected form of the data can then be used in subsequent applications, analytic engines, data transfers, and data stores, while they are readily and securely re-identified for those specific applications and users that require it.

The Challenge: Securing Sensitive Data in Big Data Ecosystems

Decision makers must have ready access to all the relevant data. Making decisions without the right data can mean the difference between a successful product introduction and a failed one. But it's not always easy to get access to all the data you need, especially where data can reside in multiple, disparate databases 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 adoption of 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. With data in constant motion and with rising threats to sensitive data from both inside and outside the enterprise, companies 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 Unified Data Architecture (UDA) is an integrated solution designed to make it easy to transform data into meaningful insights from big data environments. The Teradata UDA unifies all forms of data into an architecture that helps you achieve a 360-degree view of your data so you can make smarter decisions based on relevant insights.

Voltage SecureData for Teradata provides easy-to-configure data security capabilities you expect in an enterprise system. Authentication and authorization are just the start. Together with the Teradata UDA and 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) and secure stateless tokenization (SST) from Voltage, protection is applied at the data field and sub-field 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 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 and pseudonymization guidance in the new GDPR (General Data Protection Regulation) legislation for European Union
+ 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 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

Visit: **voltage.com**

Teradata Product Snapshot

The Teradata UDA is a powerful and complete analytics solution. By integrating the Teradata data warehouse, Teradata Aster Discovery Platform, and Hadoop into a cohesive and transparent fabric, the Teradata UDA bridges the gap between the business language of SQL and the emerging popularity of MapReduce. The result is a unified, high-performance analytics environment.

Teradata Benefits

+ Single, integrated view of the business
+ Smarter, faster decisions
+ Enable business growth
+ Competitive edge to win
+ Raising intelligence and intelligence for all
+ Platform family of appliances offers innovation

Visit: **teradata.com**

Security from the Source

Voltage SecureData is a certified technology partner with Teradata Corporation. SecureData encryption and tokenization protection can be applied at the source before it gets into the Teradata UDA, or can be evoked during an ETL transfer to a landing zone, or from the process transferring the data into the Teradata UDA or Hadoop.

Once the secure data is in the Teradata UDA or Hadoop, it 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 for more details.

How It Works

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

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

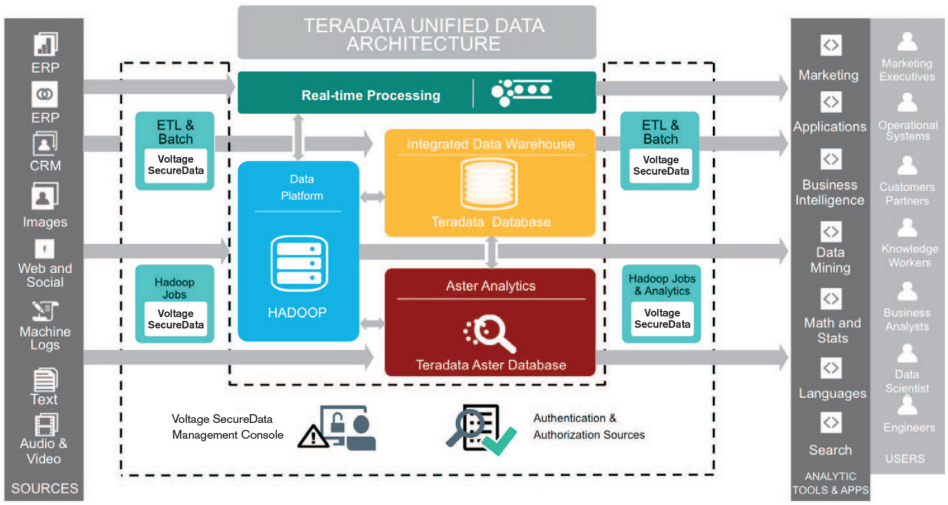

Figure 1. Voltage SecureData for Teradata

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 establish a robust, secure Teradata big data deployment.

About Teradata

Teradata helps companies get more value from data than any other company. Teradata's leading portfolio of big data analytic solutions, integrated marketing applications, and services can help organizations gain a sustainable competitive advantage with data.

Visit: **teradata.com**

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.

About Micro Focus Security

Micro Focus® is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from Micro Focus Security ArcSight, Micro Focus Security Fortify and Micro Focus Voltage Data Security, the Micro Focus Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn More At
voltage.com
microfocus.com/software/datasecurity

www.microfocus.com

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com