Securing Sensitive Data

Micro Focus® Voltage SecureData for Vertica

Voltage SecureData for Vertica Solution Snapshot at a Glance

Voltage SecureData for Vertica 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 Vertica. It also helps in significantly reducing the scope of regulatory compliance audits, such as Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA). Voltage SecureData calls for de-identifying the data as close to its source as possible, transforming the 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 readily and securely re-identified 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.
+ Data usable for many applications in its de-identified state.
+ The ability to re-identity data securely and when required—only by authorized users and applications.
+ Enable significant reduction of scope for regulatory audits such as GDPR, 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 Vertica.
+ Supports the encryption and pseudonymization guidance in the new GDPR (General Data Protection Regulation) legislation for European Union.

Vertica Big Data Platform

Vertica is an industry-leading platform for Big Data analytics. It is designed for use in data warehouses and other big data workloads where speed, scalability, simplicity, and openness are crucial to the success of analytics.

Optimized to run on-premises, on AWS, Microsoft Azure, and VMware clouds, Vertica is also available as a BYOL (Bring Your Own License) model to enable you to transition your data analytical workloads to the cloud to on premise and back seamlessly. You can also run Vertica SQL analytics engine directly on your Hadoop cluster and tap into analytics directly on ORC and Parquet data. Vertica has advanced SQL on Hadoop capabilities and achieves greater concurrency on any Hadoop distribution.

The Challenge: Securing Sensitive Data

As with any enterprise data architecture deployment, you face many security and regulatory compliance challenges, especially when automatically replicating data across multiple nodes, handling multiple types of data, or enabling access by many different users with varying analytic needs.

Sometimes the security options are not implemented in an optimal way. The most commonly cited reason for the lack of a proper security implementation is that the administration interferes with—and slows down—business due to its complex, cumbersome, and intrusive nature.

Protecting Data-in-use for Analytics—Voltage SecureData for HPE Vertica provides easy-to-configure data security capabilities you expect in an enterprise system. Authentication and authorization are just the start. With Voltage SecureData for HPE Vertica, the 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. This data-centric approach caters to the security needs of Big Data solutions such as Vertica.

With Voltage SecureData format-preserving encryption and tokenization technologies, protection is applied to the data field and subfield level. This preserves 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 protects data-at-rest, in-motion, and in-use, so the majority of analytics can be performed on the de-identified data in its protected form. Data scientists need not have access to live payment card, personal, or protected health information in order to deliver business insights.

Security from the Source

Voltage SecureData encryption and tokenization protection can be applied at the source before it gets into Big Data environments. It can also be evoked during an extract, transform, and load (ETL) transfer to a landing zone or in the process of transferring data into Vertica analytic programs. Once the secure data is in Vertica, it can be used in its de-identified state for additional processing and analysis without further interaction with the Voltage SecureData system. When needed, analytic programs that run on Vertica can securely access the clear text by utilizing the Voltage

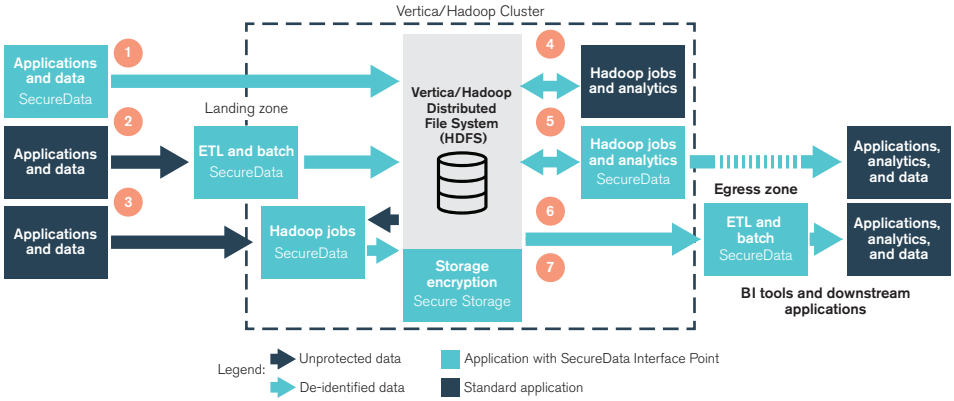

Figure 1. Options for securing data in Vertica Big Data platform

SecureData high-speed decryption and de-tokenization interfaces, with the appropriate level of authentication and authorization.

If processed data needs to be exported to downstream processing in the clear, for example, to perform actions such as customer mailings there are multiple options for re-identifying the data securely in Vertica.

How It Works

Seven specific options with Voltage SecureData that protects sensitive data used in Vertica Big Data environments are listed here.

- **Option 1:** Apply data protection at source applications
- **Option 2:** Apply data protection during import into landing zone (ETL process)
- **Option 3:** Apply data protection during Vertica import processing (for example, SQL, Sqoop, MapReduce)
- **Option 4:** Using de-identified data within Vertica
- **Option 5:** Using and exporting re-identified data from Vertica (SQL, Hive, MapReduce)
- **Option 6:** Exporting data and re-identifying outside Vertica (ETL process)
- **Option 7:** Using storage-level encryption within Hadoop

About Voltage Secure Data

Voltage SecureData drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect some of the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use, and in motion. Our solutions provide advanced encryption, tokenization, and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. Voltage SecureData solves one of the industry's biggest challenges—how to simplify the protection of sensitive data in even the most complex use cases.

Resources Visit: **www8.hp.com/us/en/softwaresolutions/big-data-platform-haven/**

Micro Focus Developer Community visit: **community.dev.hpe.com/t5/Vertica Wiki/HP-Vertica-Integration-with-HP Security-Voltage-Protecting/ta-p/227270**

Learn More At
vertica.com
voltage.com
software.microfocus.com

VERTICA

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

361-000029-001 | 4AA6-0855 | H | DS | 09/17 | © 2017 Micro Focus. All rights reserved. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

MICRO FOCUS