Hewlett Packard Enterprise

Securing sensitive data

HPE SecureData for HPE Vertica

HPE SecureData for HPE Vertica solution snapshot

HPE SecureData for HPE 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

HPE SecureData brings a unique proven data-centric approach to the protection of sensitive data in HPE 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).

HPE 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.

HPE Vertica Big Data platform

HPE Vertica is an industry-leading, comprehensive, scalable, open, and secure platform for Big Data. It transforms data into knowledge, and delivers that knowledge at the right time and place to those in the organization who need it.

HPE Vertica is available both on-premise and in the cloud. HPE Vertica OnDemand, which runs on the HPE Helion cloud, gives organizations of all sizes cloud-based access to key components of the HPE Vertica platform. Developers can also leverage this innovative Web service, as well as engage with a robust and growing community to create next-generation applications and services. Taken together, HPE Vertica platform means better, faster business insight at less cost.

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

HPE 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 HPE 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 HPE Vertica.

With HPE SecureData format-preserving encryption and tokenization technologies, protection is applied to the data field and sub-field 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. HPE 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

HPE 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 HPE Vertica analytic programs. Once the secure data is in HPE Vertica, it can be used in its de-identified state for additional processing and analysis without further interaction with the HPE SecureData system. When needed, analytic programs that run on HPE Vertica can securely access the clear text by utilizing the HPE SecureData high-speed decryption and de-tokenization interfaces, with the appropriate level of authentication and authorization.

HPE 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 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 HPE Vertica.

Resources

Visit: www8.hp.com/us/en/software-solutions/big-data-platform-haven/

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

Sign up for updates

Options for securing data in HPE Vertica Big Data platform

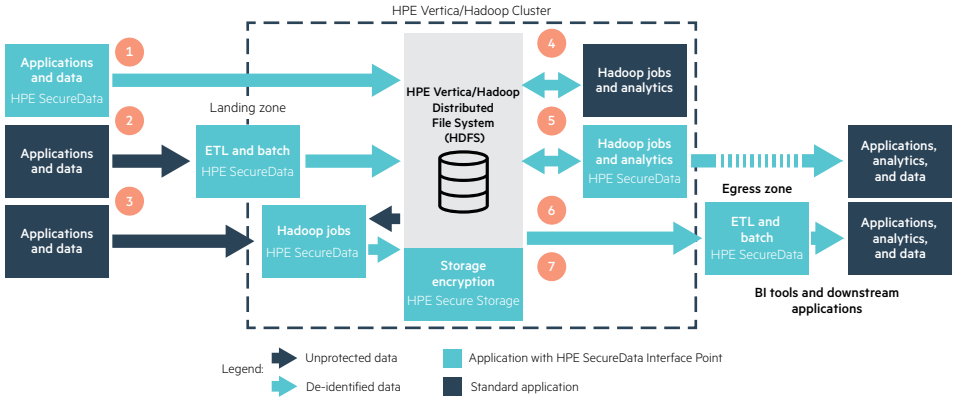

Figure 1. How it works

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 HPE Vertica.

How it works

Seven specific options with HPE SecureData that protects sensitive data used in HPE 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 HPE Vertica import processing (for example, SQL, Sqoop, MapReduce)
- Option 4: Using de-identified data within HPE Vertica
- Option 5: Using and exporting re-identified data from HPE Vertica (SQL, Hive, MapReduce)
- Option 6: Exporting data and re-identifying outside HPE Vertica (ETL process)
- Option 7: Using storage-level encryption within Hadoop

About HPE Security — Data Security

HPE Security — Data Security 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. HPE Security — Data Security solves one of the industry's biggest challenges—how to simplify the protection of sensitive data in even the most complex use cases.

Learn more at
voltage.com
hpe.com/software/datasecurity

Hewlett Packard Enterprise

4AA6-0855ENW, June 2016, Rev. 1