

Voltage SecureData Integrations for Snowflake

Enabling high-scale, high-performance, and secure data analytics, data science and data sharing.

Key Benefits

Voltage SecureData Enterprise enables secure analytics by applying data-centric protection within the existing schema of a data store. SecureData preserves a protected dataset's

enterprises can benefit from Many companies that have invested in expensive on-premises data warehouse systems, Hadoop data lakes, and their surrounding ecosystems have shifted their data into the cloud.

Why? The cost-effectiveness of cloud storage and its ever-increasing array of services enable organizations to get more value from monetizing their rapidly expanding data volumes in these large-scale environments.

However, as demonstrated by an almost continuous stream of reports, cloud-related data breaches are not likely to decline. So, amid these very insistent demands for cloud adoption from the business side, data security nevertheless remains a board-level concern. Voltage SecureData Enterprise can help customers ensure that the adoption of cloud services, like the Snowflake Data Cloud, doesn't result in a breach of sensitive data, (such as PII, PCI, PHI, and intellectual property), corresponding regulatory fines, or damage to brand, reputation, and customer trust.

* Gartner. (2021, November 10). Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences [Press release]. www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

Product Highlights

How Voltage Data Privacy and Protection Can Help

The OpenText™ Cybersecurity Voltage Data Privacy and Protection framework includes critical capabilities from [data discovery](#) to [disposition](#). Understanding the flow, use, and storage of data is key to compliance in today's era of global privacy legislation. Organizations need practical tools to find data within the scope of privacy policies, automate tagging and enrichment of metadata, identify data subject information, and to assess risk.

Voltage Data Privacy and Protection provides solutions that discover, analyze, and classify all data, [whether structured, semi-structured, or unstructured](#). Policies covering the entire data lifecycle allow enterprises to act on their data with contextual awareness and deep insights from rich risk profile visualizations. Voltage SecureData Enterprise in particular uses standards-validated, [data-centric](#) security innovations to pseudonymize and anonymize sensitive information, to deliver persistent privacy for data wherever it resides, moves, or is used.

Voltage SecureData Integrations for Snowflake Benefits

The Snowflake platform provides several native, layered security options, including network security, identity and access management, transparent disk encryption, TLS, and standard data-at-rest encryption. Voltage SecureData Enterprise adds important [data-centric](#) protection options that enhance data security in the Snowflake Data Cloud in several critical ways:

- Format-preservation for the usability of data in its protected form
- Data security controls for data privacy regulation compliance
- Persistent protection enabling multi-cloud and data sharing strategies
- Flexibility of standards-validated and independently assessed techniques
- Safe unicode support for all alphabets

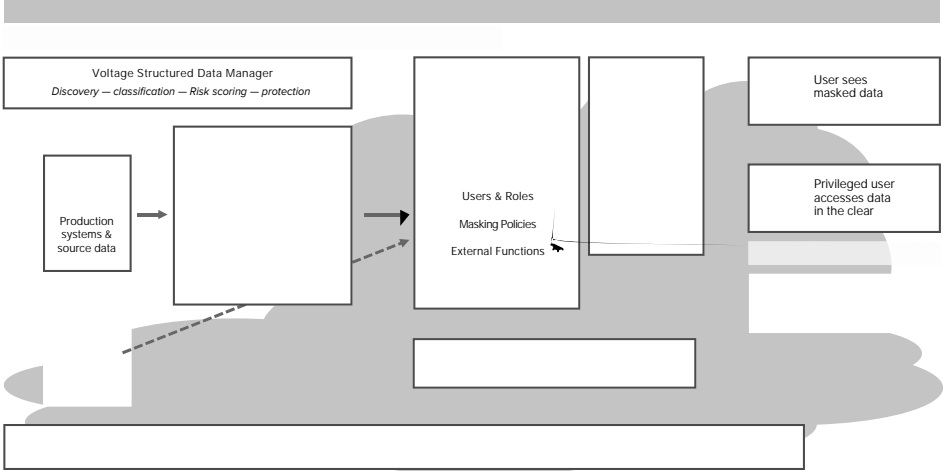
Data protected by Voltage SecureData Enterprise's range of [tokenization technologies](#) retains its referential integrity, enabling customers to perform data analytics upon protected data sets. Voltage SecureData Enterprise preserves data formats so that the protected form of the data fits seamlessly into existing table schema. Reversible and irreversible methods for sensitive data types across all languages are provided. These methods include format-preserving [encryption](#) (FPE), secure stateless tokenization

(SST), and format-preserving hash (FPH) that enable customers to pseudonymize and anonymize data, as required, wherever it is or wherever it must go.

In addition, the mobility of data protected by Voltage SecureData Enterprise is unconstrained: data remains protected while flowing into or out of Snowflake, from or to other cloud services or cloud platforms. This approach supports a [multi-cloud strategy](#) and data sharing requirements without requiring organizations to compromise on data security at the boundaries of these services. And with [Voltage SecureData Enterprise](#), you always remain in complete control of your encryption keys and token

Key Features

Reference Architecture



“Our clients want to lock down their sensitive data,
but still be able to unlock the value in that data at scale.”

Head of Cybersecurity Practice
Global Systems Integrator



for extended first-party, second-party,
and third-party analytics. In other words,
Voltage SecureData Enterprise Integrations
for Snowflake enables you to lock down
your sensitive data but still unlock the
value in that data at scale.

Learn more at
[www.microfocus.com/en-us/cyberres/
partners/snowflake](https://www.microfocus.com/en-us/cyberres/partners/snowflake)