OpenText Data Privacy and Protection Integrations (Voltage) for Snowflake

Secure analytics with data privacy and protection

OpenText Data Privacy and Protection Integrations for Snowflake at a glance

- Strong protection for data at rest
- Analytics executed on protected data at scale
- Protect sensitive PII, PCI, PHI and intellectual property data in Snowflake
- NIST-standard Format-Preserving Encryption, tokenization, hashing, and data masking
- Maintain complete control of cryptographic keys
- Pseudonymize data in Snowflake for privacy and regulatory compliance
- Integration enables 100% cloud-native solution for high-scale secure cloud analytics

High-scale secure cloud analytics with Snowflake

OpenText collaborates with Snowflake to deliver data-centric protection to organizations worldwide. The integration of OpenText™ SecureData (Voltage) with Snowflake Data Cloud enables OpenText customers to shift workloads seamlessly and securely to Snowflake without the risk of compromising business-sensitive data, while adhering to privacy regulations. The integration also helps customers of Snowflake acquire secure data analytics capabilities offered by OpenText SecureData.

Snowflake's platform enables a wide variety of workloads and applications on any cloud, including data warehouses, data lakes, data pipelines, and data sharing as well as business intelligence, data science, and data analytics applications.

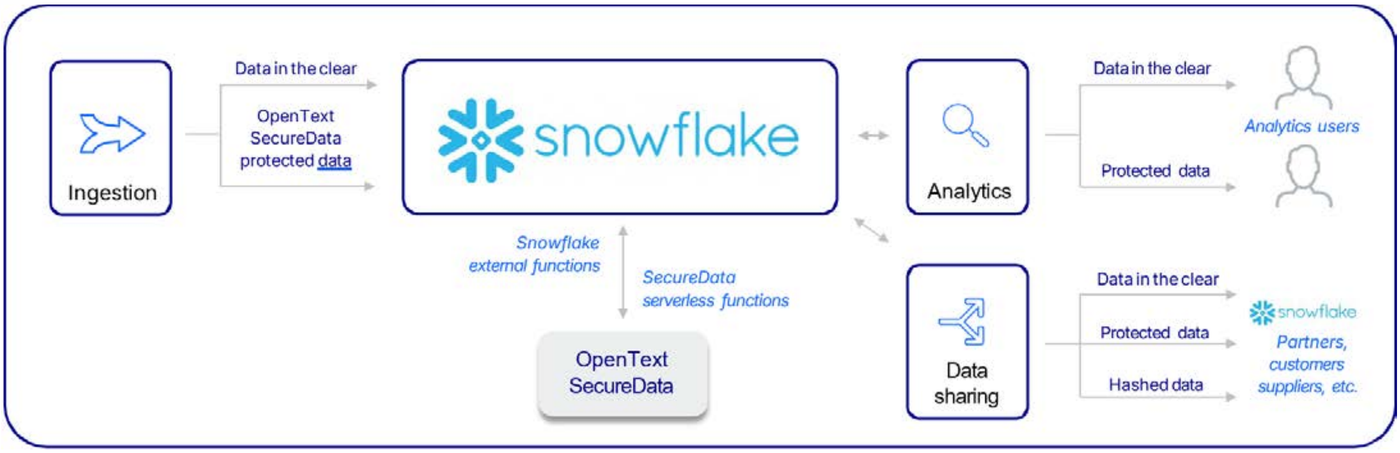
This powerful, integrated solution adds a 100-percent cloud-native solution for high-scale secure cloud analytics to OpenText SecureData's deep capabilities for data privacy and protection across databases, data warehouses, and big data environments.

The need to secure sensitive data in Snowflake Data Cloud

The protection and privacy of sensitive data is a critical responsibility for organizations worldwide. The risks of data breach and regulatory compliance violation continue to rise, and receive board-level attention and accountability. Global organizations are expanding the scope of their data protection policies.

In addition to the familiar PCI, PII, and PHI data types that require strong protection, it is common that geolocation data, intellectual property data, and transactional data are now also subject to increased security and control. As global organizations lift and shift workloads to the cloud, data analytics and data science rise to the top of their priority lists. Drivers for cloud migration include financial benefits like pay-per-use, operational benefits like zero maintenance, IT modernization with reduced need for capacity planning and management, and technical benefits like easy availability of third-party data streams. There is unmet demand from the business as on-premises data centers only serve a small percentage of the actual demand for data analytics. Platforms for machine learning and artificial intelligence are readily available in the cloud and offer the potential to discover new value and insight using large stores of business data.

But with the migration to cloud comes new challenges. Organizations are struggling to define the appropriate level of protection and privacy for sensitive data in the cloud, and these challenges are heightened by the fractured nature of cloud controls. Each cloud service provider brings its own approach to key management, identity access management, storage-level encryption, and application-level policy management. Most organizations are using multiple cloud providers, complicating efforts to protect sensitive data moving across hybrid IT. Under the shared responsibility model, cloud providers will ensure that the hardware and software services they offer are secure, but the business customer is responsible for the security of its own data assets.



OpenText SecureData solves new business challenges

OpenText Format-Preserving Encryption (FPE), a mode of the Advanced Encryption Standard (AES), is a fundamental innovation which enables OpenText SecureData to provide high-strength, robust data encryption, while maintaining flexibility for use. OpenText FPE provides the pseudonymization necessary to enable compliance with data privacy regulations at data field and sub-field levels, while simultaneously enabling organizations to run business processes and analytics on protected data sets.

OpenText FPE maintains the context and meaning of the data—such as its referential relationships, logic, and business intent—in its protected form, ensuring that businesses can minimize requirements to decrypt. Maintaining referential integrity enables shared analytics use cases which are impossible using traditional masking or randomization approaches. The preservation of referential integrity also enables protected data to be reliably referenced and joined for cross-cloud analytics, providing key insights through identifiers, such as phone numbers or IDs, common across disparate data sets.

Snowflake and OpenText SecureData enable a 100% cloud-native solution for high-scale secure cloud analytics.

Using Snowflake and OpenText SecureData together, organizations can protect any structured data type, in any quantity required. Analytics, data science, and data sharing are not impacted by the security controls as the combined solution can enable the use of any query tool or business intelligence platform with no change to SQL syntax and minimal impact on performance. OpenText SecureData offers a comprehensive choice of techniques including encryption, tokenization, and hashing to protect data—supporting many different use cases and compatible with OpenText SecureData's dozens of other platform clients, from mainframe to mobile.

The protection technologies in OpenText SecureData provide flexible implementation and data-centric protection for a virtually unlimited number of structured data types in any language, and any region, with proven performance, reliability, and scalability.

Protecting data privacy and enabling secure cloud analytics in Snowflake

OpenText SecureData provides all of these capabilities without impacting investments in analytics, data science, or business intelligence infrastructure. OpenText SecureData helps organizations strengthen their cyber resilience by providing an end-to-end data-centric approach to enterprise data protection. Customers of the integrated OpenText SecureData + Snowflake Data Cloud solution can lock down their data against theft or accidental exposure while also being able to unlock the value of their data, at scale.