cpl.thalesgroup.com

THALES

Securing Sensitive Data and Addressing Compliance for SingleStore Databases

The Problem: New Cloud Native Database Technology Still Stores Sensitive Data in Need Of Security

With more data of varying formats available in real time, organizations use a variety of solutions from databases to message brokers to help aggregate and analyze this data to better run their businesses. The challenge for organizations is to analyze and act on their data as quickly as possible. Unfortunately, each solution that is added to the process – whether a database for a specific data format or an analytics tool – slows down the time to value. SingleStore addresses this challenge by offering customers a cloud native, distributed database that allows organizations to quickly ingest and analyze a variety of data formats from a wide range of sources.

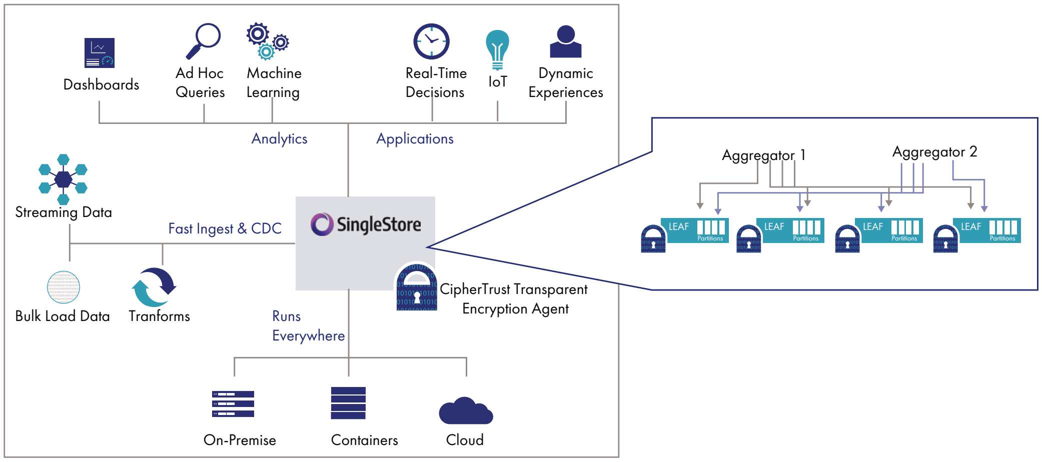
Despite these advancements in database technology, traditional security concerns remain. Much of the data that SingleStore customers hold is highly sensitive data often falling under specific compliance obligations. As a central repository for sensitive data, databases are often prime targets for anyone wanting to take advantage of sensitive data, especially those individuals with privileged access. In addition, many industry regulations explicitly require encryption and external key management of specific data categories. Complicating these concerns is the prospect that this data will be held in public cloud technology with operations spread across geographic regions. Combined, organizations have quite a few considerations to address in order to adopt SingleStore in a secure and compliant manner.

SingleStore

The Solution

CipherTrust Transparent Encryption (CTE) secures SingleStore DB data-at-rest at the file system-level and uses centralized key management, privileged user access controls and detailed data access audit logging for more robust data security. With CTE, customers can secure their SingleStore data wherever it resides whether on-premises or in the public cloud.

Organizations can deploy CTE quickly, simply, and scalably. CTE agents install on the same operating file-system or device layer as SingleStore DB and define which directories are to be encrypted. Since it occurs at the file-system layer, encryption and decryption remain transparent to SingleStore DB and all applications meaning that organizations do not have to make architecture changes or plan for downtime to secure their data. Addtionally, CTE's performance impact on SingleStore DB operations is negligible (typically 0 to 3 percent). CTE's file-system level encryption addresses a wide range of data security compliance and best practice obligations with minimal disruption. CTE works together with the CipherTrust Manager, a FIPS 140-2 up to Level 3 validated centralized encryption key and policy platform.



Why Use Thales CipherTrust Transparent Encryption

Combining SingleStore DB with CTE lets organizations secure a wide range of data formats from a broad array of sources while still keeping it all available to drive business value quickly. By using Thales' CipherTrust centralized key management, organizations can easily incorporate their SingleStore DB deployment into their larger organization-wide crypto strategy. Additionally, CTE's policy-based privileged user access controls and audit logging separate database security and system administration responsibilities to increase security oversight and ultimately improve effectiveness and satisfy key compliance obligations.

Simplified Deployment and Administration

Ciphertrust Transparent Encryption minimizes the time and effort required to implement and maintain data at rest security for SingleStore DB. CTE's implementation does not require application or database code or architecture changes making security an easy addition. Moreover, CipherTrust Manager serves as a consolidated, central management plane for encryption keys and policies for SingleStore DB and a wide range of enterprise storage, database and application security solutions.

Granular User Access Policy Controls and Enforcement

CTE has the ability to define and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to SingleStore DB. Such policies allow specific individual users and processes access to data in clear-text while restricting the file system commands they can perform. Access controls serve as an additional layer of protection between data and systems that makes data safer. Using these access controls, organizations can allow system administrators to manage configurations and ongoing maintenance without having clear-text access to sensitive SingleStore data.

Comprehensive Compliance Controls and Audit Trails

CTE's detailed data access audit logging addresses many common regulatory compliance controls for encryption, data sovereignty, least-privileged policy and data access auditing. Auditors use intelligence logs to assess the effectiveness of encryption, key management and access policies. Logs reveal when users and processes access data, under which policies, whether requests were allowed, and even when a privileged user submits a command like "switch user" to attempt to imitate another user. Additionally, CTE's pre-built integration to leading Security Information and Event Management (SIEM) systems mean this log data is available for use to provide immediately actionable insights.

Key Benefits:

- Robust file-system-level data encryption
- Customer controlled centralized key management
- Granular policy-based privileged user access controls

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments.

About SingleStore

SingleStore is a distributed, highly-scalable SQL database that can run anywhere. It delivers maximum performance for transactional and analytical workloads with familiar relational models.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or https://www.singlestore.com/