How ScyllaDB Cloud Protects Your Sensitive Data

> *"Dance like nobody is watching. Encrypt like everyone is."*
> – Werner Vogels, CTO of Amazon

This paper explores the encryption measures that ScyllaDB Cloud takes to help our customers protect sensitive data in their database clusters. We summarize how database-level encryption at rest features can help in the battle for customer data protection—bringing information security to the next level.

Sensitive Data

Personal Sensitive Data

In the last decade, we have heard a lot about personally sensitive data and its protection. What makes it so unique?

'Personal sensitive data' refers to information that, if leaked or misused, may cause a significant threat, harm, or discrimination against individuals. Personal sensitive data includes:

- Personally identifiable information (PII): Names, addresses, social security numbers, biometric data, etc.
- Health information: Medical records, diagnoses, treatment plans.
- Financial data: Bank account details, credit card numbers, income information.
- Other sensitive categories: Religious beliefs, political affiliations, and sexual orientation.

Corporate Sensitive Data

Media pays less attention to corporate sensitive data, a precious asset that can make or break a company's fortunes. Any exposure of this data can lead to substantial damage, both financial and reputational.

Companies maintain the security and protection of corporate and private sensitive data at all times.

The biggest challenge in protecting the data is identifying all places containing sensitive data. Some companies report users might store sensitive data in any database or table, making data protection nearly impossible to govern.

Databases predominantly store all data, including sensitive data. Database entries are always a potential target for attacks from malicious actors. As a robust NoSQL database, ScyllaDB offers various encryption options that work well together to protect customer sensitive data.

ScyllaDB Cloud - Encrypted by default

ScyllaDB Cloud encrypts storage and also runs database-level encryption to encrypt the data before it hits the database. This ensures customer data is secure and adheres to all privacy regulations.

By default, encryption uses the symmetrical algorithm AES-128, a solid corporate encryption standard covering all practical applications.

Breaking AES-128 can take an immense amount of time, approximately trillions of years.

If needed, the strength can be increased to AES-256, which is the US government's strongest requirement. The theoretical time to break AES-256 is septillion (1024) years.

Note: At the time of publication, database-level encryption in ScyllaDB Cloud is available for all clusters deployed in Amazon Web Services. We plan to extend support for the other supported cloud service providers.

Encryption at rest

Encryption at rest is when data files are encrypted before being written to persistent storage. ScyllaDB Cloud always uses encrypted volumes to prevent data breaches caused by physical access to disks.

Modern security breaches happen primarily because of human errors, compromised applications, or compromised system security. Research shows that one or a combination of more of those problems caused 58% of all breaches.

To help customers improve information security, ScyllaDB Cloud offers database-level encryption at rest by default. Since our latest release, we have made it the default for all newly created clusters.

Database-level encryption

Database-level encryption is a technique for encrypting all data before storing it in the database. The cloud feature is based on ScyllaDB Enterprise Database-level Encryption at rest.

The data remains encrypted at all times. Even if a malicious actor gains access to it, they cannot decrypt it without a decryption key.

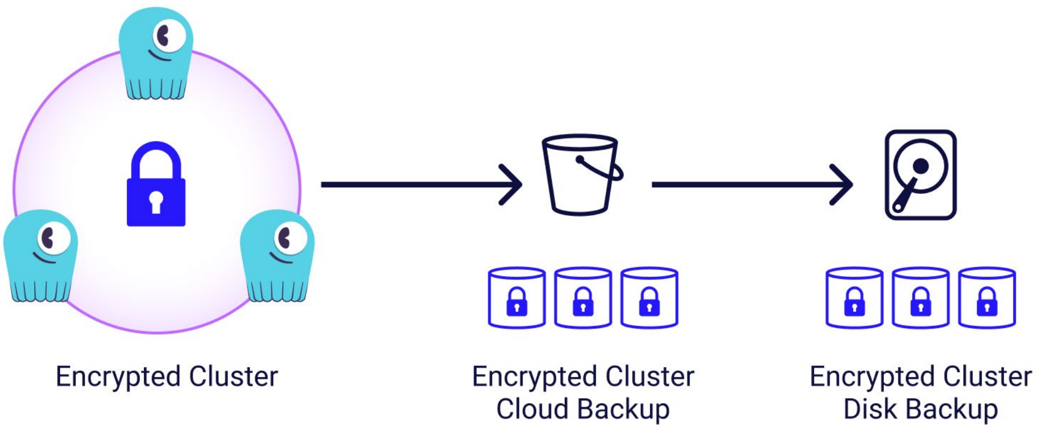
The system stores and protects the keys separately from the database, substantially increasing security.

To ensure all user data is protected, ScyllaDB Cloud will encrypt:

- All user tables
- Commit logs
- Batch logs
- Hinted handoff data

This covers all locations where customer-sensitive data can be located, temporary or permanent.

Database-level encryption has another strong protection mechanism. Typically, every copy of the data creates another vector of attack. Because the data itself is encrypted, all copies of the database files contain only encrypted data and are, therefore, automatically protected.



The archive data can only be decrypted by the same master key, which is protected securely. Without the key, all the data will remain encrypted.

Customer Managed Keys (CMK)

ScyllaDB Cloud provides complete database-level encryption using the Customer Managed Keys (CMK) concept. It is based on the envelope encryption cryptography technique. A key feature of CMK is that the master key's owner has full control over encrypted data access. Without the master key, no one can decrypt the data.

Control over the data encryption.

ScyllaDB Cloud puts strong encryption tools directly in the hands of its users. The combination of database-level encryption and Customer Managed Keys gives businesses full control over the security of the data they handle. This comprehensive approach ensures that the entrusted data remains protected throughout its lifecycle, instilling trust and confidence in the operations.

By controlling the master key, users can:

- Revoke data access at any time.
- Restore data access at any time.
- Rotate the master keys to increase the security.
- Log all access attempts to keys and data.

Even make the data permanently encrypted in all copies by destroying the key.

ScyllaDB Cloud database-level encryption ensures that:

- Even if the data gets compromised, the information remains secure.
- All data in backup files is encrypted and protected.
- Since the key never leaves the key store, the KMS will log every attempt to decrypt the data.
- The possibility of exposing data by human error is limited. Keys and data require different levels of authorization.

- Full database-level encryption helps to meet recommendations from regulatory standards like
  - General Data Protection Regulation (GDPR)
  - Health Insurance Portability and Accountability Act(HIPAA),
  - PCI Data Security Standards (PCI DSS)
  - California Consumer Privacy Act (CCPA)

  which always recommend full data encryption.
- Even in the unlikely event that a database cluster or the application is exposed, customers can independently revoke any access to the data.

ScyllaDB Managed Service

ScyllaDB Cloud offers a fully managed service to support and manage customer database clusters on the customer's behalf.ScyllaDB can create, manage, and assign database encryption keys on the customer's behalf.

It is a peace-of-mind option. Our customer success agents manage access to the data and can assist with encryption/decryption or revoking access if needed. It makes life easier while providing security and control.

ScyllaDB Privacy and Compliance

ScyllaDB fully commits to transparency in how we collect, use, and protect data received by ScyllaDB. Please refer to the ScyllaDB Privacy Policy and ScyllaDB Policies and Agreements for more information.

ScyllaDB undergoes independent third-party audits to confirm that it meets strict industry standards for security, availability, processing integrity, confidentiality, and privacy.

ScyllaDB meets the compliance requirements of the following standards, as certified.

Cost-effective protection

According to a Cost of Data Breach report by Ponemon Institute, the average data breach cost was $4.5 million in lawsuits, settlements, or paid ransoms. Just for reference, that's $165 per record.

The performance impact of database-level encryption at rest is very low—less than 5% of computing on average. It has minimal impact on storage and latency performance.

The AWS KMS will cost $1/month for each cluster prorated per hour. Each additional data center creates a replica that is counted as an additional key.

There is an additional cost per key request. ScyllaDB Enterprise efficiently utilizes those, resulting in an estimated cost of 0.06 cents per month for a 9-node cluster. For every 3 nodes, the cost of key requests will increase by $0.02 per month.

ScyllaDB Database-level encryption

ScyllaDB Cloud implements measures in advance to protect sensitive data. The information stays protected and under the customer's control through database-level encryption at rest and customer-managed keys.

Knowing that their critical assets are encrypted, businesses can focus on their core operations.

For more information, see:

[Getting Started with Database-Level Encryption at Rest in ScyllaDB Cloud]

Start using this feature in [ScyllaDB Cloud].

We welcome your questions in our [community forum] and [Slack channel].

Alternatively, you can reach us via [this contact form].

ScyllaDB is the database for data-intensive apps that require high performance and low latency. It enables teams to harness the ever-increasing computing power of modern infrastructures—eliminating barriers to scale as data grows. Unlike any other database, ScyllaDB is built with deep architectural advancements that enable exceptional end-user experiences at radically lower costs. Over 600 game-changing companies like Disney+ Hotstar, Expedia, FireEye, Discord, Crypto.com, Zillow, Starbucks, Comcast, and Samsung use ScyllaDB for their toughest database challenges. ScyllaDB is available as free open source software, a fully supported enterprise product, and a fully managed service on multiple cloud providers.

ScyllaDB

United States Headquarters
1309 S. Mary, Suite 219,
Sunnyvale, CA, 94087 USA
Email: info@scylladb.com

Israel Headquarters
11 Galgalei Haplada
Herzelia, Israel

Copyright © 2024 ScyllaDB Inc. All rights reserved.
All trademarks or registered trademarks used herein
are property of their respective owners.