WELCOME

Queryable Encryption

Run expressive queries directly on encrypted data

Tom Slattery
Solutions Architect

MISSION CRITICAL

Built-in security. Proven data protection.

Trusted for mission-critical workloads

Banks, healthcare organizations, and government agencies trust MongoDB to run applications at the core of their business.

Security isn’t just a checkbox

It’s woven into every stage of our development lifecycle.

Continual security investment

To develop new capabilities that help customers protect their most sensitive data with confidence.

Advanced encryption

Enables protection throughout the data lifecycle

MongoDB is uniquely positioned to protect your data through every stage of its lifecycle.

Encryption throughout the data lifecycle

In-Transit

Protects data while it is being transferred across networks to prevent interception

At-Rest

Secures data when it is stored on disk or in databases to safeguard against unauthorized access.

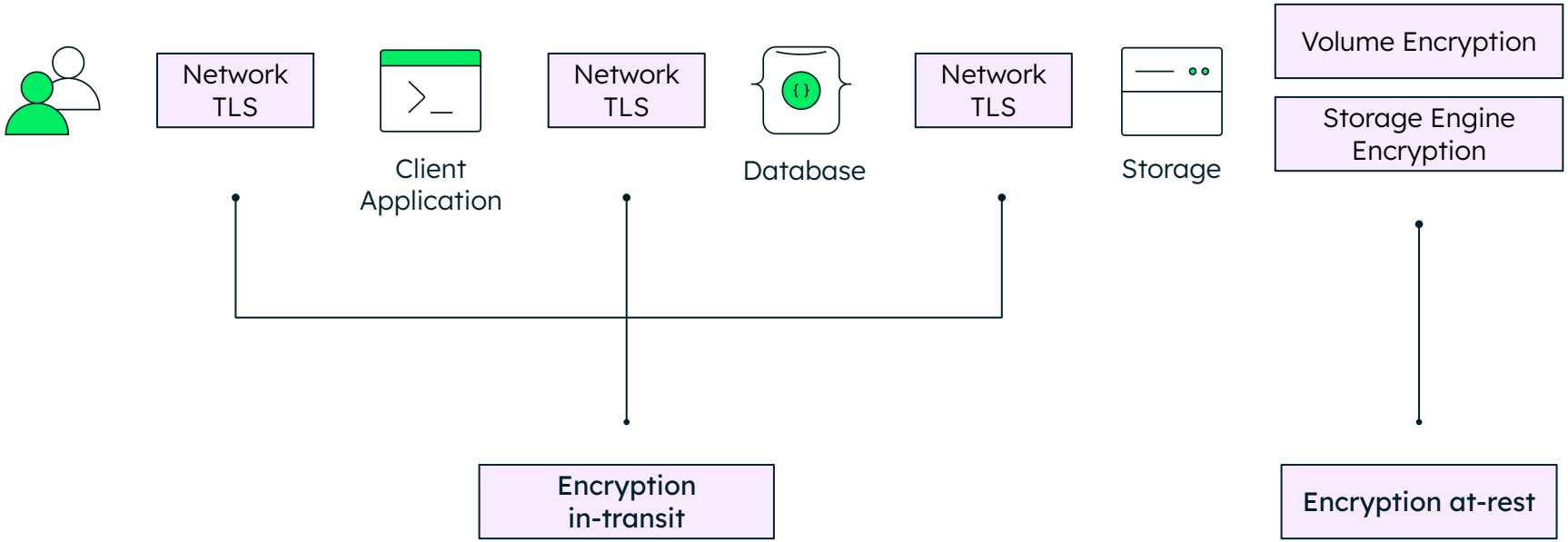
In-Use

Protects data during active processing or computation to ensure it remains secure while being accessed.

True protection and compliance require all three types of encryption.

Data in-transit & at-rest:

Most databases have it covered!



What about data in-use?

- Encryption in-use is difficult because encrypted data is unreadable.
- Databases traditionally cannot query encrypted data without first decrypting it.
- If the database lacks the decryption key, data must be sent back to the client for decryption, which does not scale.
- Decrypting data increases the risk of exposure by making sensitive information accessible.

Stuck between a rock and a hard place

1. Do nothing and risk unencrypted data in use within a live database **being exploited**, leading to an unauthorized disclosure
2. Rely on third-party tools and/or custom-built encryption implementations to protect data in use, leading to **more complexity** and **less security**

Client-Side Field Level Encryption (CSFLE)

Select an encryption key, configure the fields to be encrypted in the MongoDB driver... and **GO**

- Sensitive data never **leaves the application** without first being encrypted
- No need to **modify applications**
- Data is **still queryable** ***(equality query)***
- **Minimal performance impact** to the database

Benefits of in-use encryption

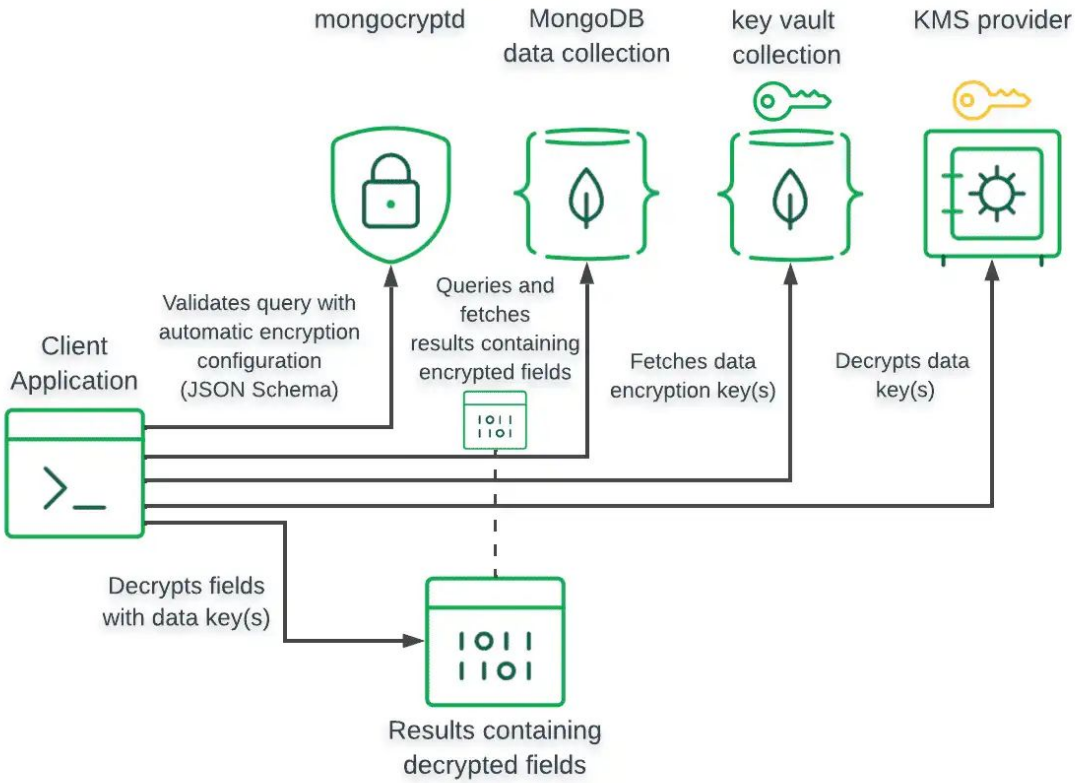
Separated from the database
Sensitive fields are encrypted by the drivers before data leaves the app.

Protection throughout data lifecycle
Data in memory, logs, storage and backups stays encrypted.

Inaccessible to admins
Data can only be decrypted by a party that has client access or network & database access AND the decryption keys.

Flexible, field-level control
Encrypt one field, multiple fields, or entire documents, each with their own key.

Read Data From Encrypted Fields



INDUSTRY-FIRST

MongoDB Queryable Encryption

A **one-of-a-kind** in-use encryption technology **protects sensitive data** when it stored, processed and queried – throughout its lifecycle. It allows applications to encrypt sensitive data on the client side, securely store it in the MongoDB database, and **perform expressive queries directly on the encrypted data**.

PIONEERING

MongoDB Cryptography Research Group

Seny Kamara

Head of Research

Tarik Moataz

Principal Research Scientist

Comprised of the **world's leading** cryptography and encrypted search researchers and scientists.

Applied **years of pioneering research** to develop Queryable Encryption.

Research behind Queryable Encryption is **published and reviewed** by top cryptographers worldwide.

Outcomes

Strong data protection

Data stays encrypted at every stage—whether in-transit, at-rest, or in-use—reducing the risk of sensitive data exposure.

Stringent regulatory compliance

Provides the necessary tools to comply with data protection regulations like GDPR, CCPA, and HIPAA by ensuring robust encryption at every stage.

Streamlined operations

Incorporates advanced encrypted search without requiring costly custom solutions, complex third-party tools, or even application code rewrites.

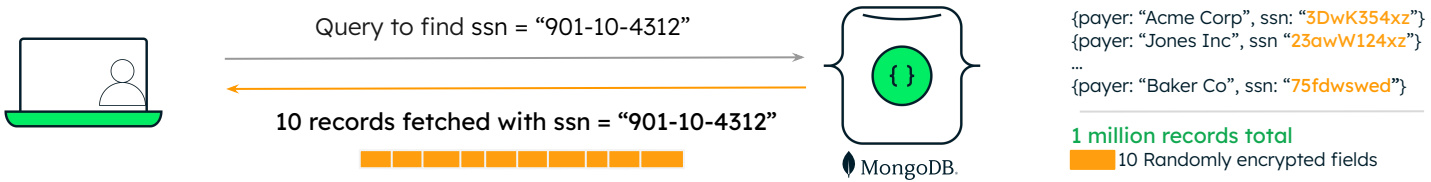
Secure performance at scale

Enables partial-text queries on encrypted field with minimal latency impact, preserving responsive user experiences even as security requirements increase.

Queryable Encryption

- Encrypt the sensitive fields
- Easy development cycle
- No cryptography experience required
- Data encrypted throughout its lifecycle
- Equality and range queries

- MongoDB is the only platform to implement a fast, searchable encryption scheme with an algorithmic approach under a well defined threat model and rigorous security guarantees.
- Server-side processing of encrypted data
- Server does not know the data



Ability to query the encrypted data with Queryable Encryption

Supported query types

EXISTING SUPPORT	**Equality**	Retrieve a record for a customer with the exact encrypted email address “alex@example.com”.
EXISTING SUPPORT	**Range**	Find all encrypted salaries between $80,000 and $120,000.
NEW	**Prefix**	Find all customers whose surnames begin with “Mac”.
NEW	**Suffix**	Match the last four digits of an encrypted Social Security number, like “-1234”.
NEW	**Substring**	Search for a keyword like “engineer” within a free-text encrypted job title or description.

SENSITIVE DATA

Ideal Queryable Encryption workloads

Highly sensitive data

Includes PII, PHI, or financial data such as names, addresses, SSNs, medical histories, prescriptions, bank account details, etc.

Compliance required

Data is subject to privacy/protection regulations such as GDPR, CCPA, HIPAA, etc.

Data residency requirements

Strict control is required over where encrypted data is stored and processed to meet regional or organizational residency mandates.

Use cases

PII Search:

- Personally identifiable information is protected under regulations like GDPR and HIPAA. With prefix query support, Queryable Encryption enables secure search without decrypting data. For example, retrieving all users whose last names begin with “Mac” or email addresses that start with “jane.”

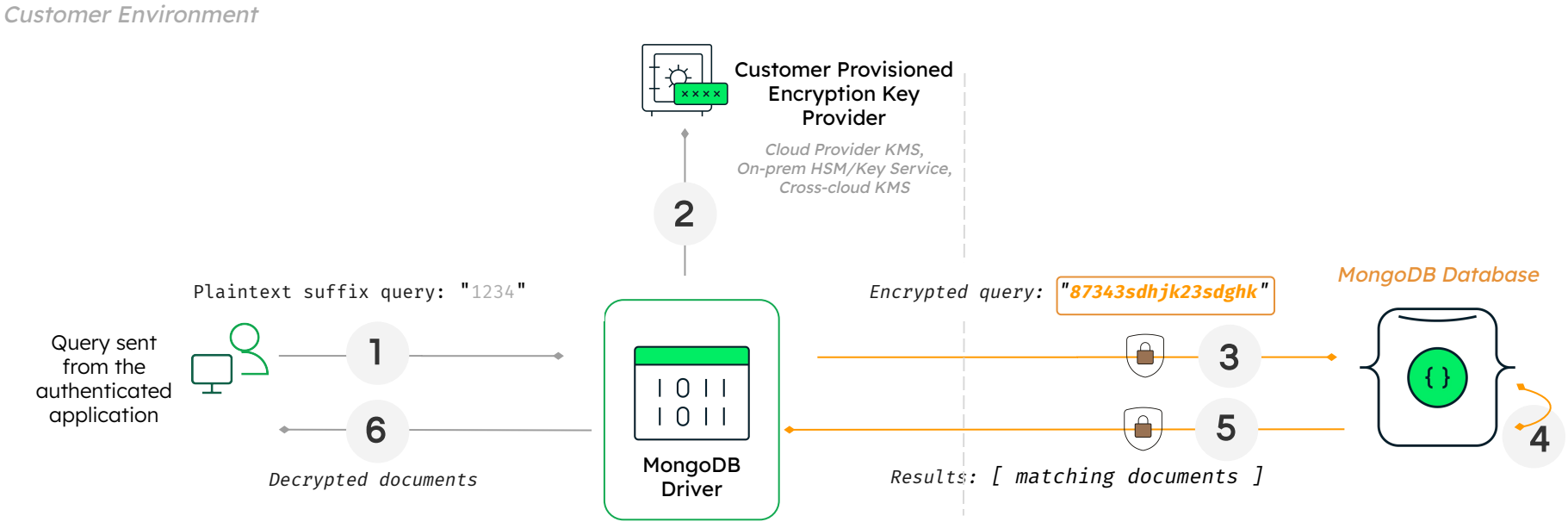
Keyword Search in Support Notes:

- Customer service notes often contain sensitive details in free-text fields. With substring query support, teams can securely search encrypted notes of up to 60 characters for keywords such as “refund,” “escalation,” or “urgent,” without exposing the contents of those notes.

Social Security Number Validation:

- Social Security numbers and other ID values are highly sensitive and regulated. With suffix query support, customers can match on the last four digits of an encrypted SSN, which are common in identity verification workflows, without revealing the full value or decrypting the field.

Example: Social Security Number validation



Encrypted data is *always* stored, transmitted, queried, and retrieved in encrypted format

How is this different than other solutions?

Microsoft Always Encrypted

Relies on hardware enclaves for expressive queries, requiring ongoing trust in the enclave vendors and in Azure.

PostgreSQL

Has no native client-side encryption.

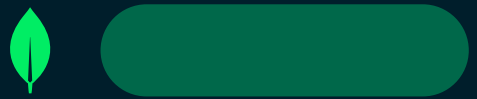
3rd Party Libraries

Some use deterministic encryption for exact matches, limiting security, while others aren't feasible for production workloads (homomorphic encryption) or are not shown to be secure (ad hoc schemes).

MongoDB CSFLE

Client-Side Field Level Encryption uses deterministic encryption for exact matches.

*Queryable Encryption is the **only solution** that operationalizes secure, performant searchable encryption. Our approach is **algorithmic and open source**, requiring **no trust relationship** with anyone.*



Thanks!
Q & A