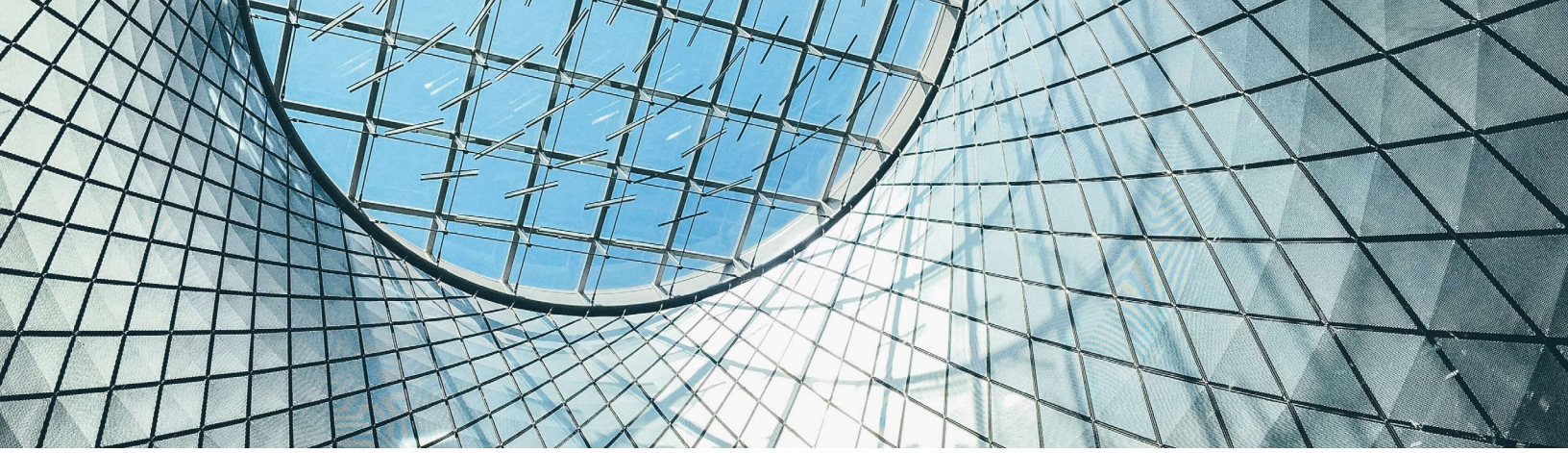

Market Insight Report Reprint

MongoDB adds security seasoning to further distinguish core MongoDB from other NoSQL fare

July 11 2022

by Justin Lam

Rather than creating separately sold security add-ons, MongoDB has chosen to build in data security features to enhance its overall platform adoption. New security features such as Queryable Encryption are integral to MongoDB and its entire OSS community, and provide a window into MongoDB's broader strategy.

451 Research

S&P Global
Market Intelligence

Introduction

For many databases and stores of information, data security has traditionally been reactively added. As the risk of storing, collecting and processing sensitive information continues to climb, existing platform vendors have developed and marketed security add-ons to their core offerings, not only as an upselling motion, but potentially as a costly cross-selling motion. With separate security sales personnel overlapping core offering sellers, platform providers often targeted enterprises differently, triangulating the security and infrastructure personas to drive adoption for their individual offerings.

Larger platform players may have chosen this strategy to enable security as a separate P&L, with the risk of internal and external seller conflict. To maximize security adoption, MongoDB has chosen the opposite, incorporating new security features into all versions of its releases, including open-source software distributions. MongoDB's latest improvements, such as Queryable Encryption, are forward-looking, incorporating privacy-enhancing technologies to enable novel data collaboration and analysis while data remains encrypted.

THE TAKE

MongoDB's approach to building security directly into its platform is worthwhile, since it removes commercial barriers to the system design principles of "secure by default, secure by design." Positioning the company as a whole to meet this design goal greatly clarifies the go-to-market message, while better appealing to development, infrastructure and security customer stakeholders. Over time, MongoDB has incorporated auditing, authentication and stronger security defaults into its releases, with newer additions in data sovereignty and security assurance for its Atlas SaaS offering. MongoDB continues this trend with Queryable Encryption. Developers can use Queryable Encryption with no alterations to document storage or subsequent queries. This kind of consistent developer experience enables not only better security outcomes, but also better development outcomes for regulated or sensitive applications.

Context

First released in 2009, MongoDB is now one of the most popular NoSQL databases. With its open-source foundation, it has become integral to the M.E.A.N. developer stack, and describes itself as a developer data platform. With over 265 million downloads and 35,000 customers, the company now earns most of its revenue via its SaaS offering, Atlas. With all these changes, table-stakes security features such as authentication, authorization and encryption-in-transit are consistently available for all distributions, including MongoDB Community editions.

Although many security features have been developed by core MongoDB staff, Queryable Encryption is based on the cryptographic research of Seny Kamara and Tarik Moataz. Kamara and Moataz founded Aroki Systems, which pioneered the underlying mechanics of Queryable Encryption. Since then, MongoDB has acquired Aroki. Kamara and Moataz are also co-directors at the Encrypted Systems Lab at Brown University. Kamara and Moataz now lead MongoDB's Advanced Cryptography Research Group to develop additional security and privacy enhancing technology.

Technology

MongoDB has directly added security features to its platform. It has largely focused on the MongoDB-specific implementation of these features while adhering to standards for orchestration and auditing. Simply put, MongoDB's security features are implemented at the data platform layer, with extensibility to larger control planes in authentication, origination, authorization, orchestration and audit. For example, MongoDB Atlas relies on external key management services such as Azure Key Vault or AWS KMS.

Queryable Encryption extends data-at-rest encryption closer to a never-decrypted ideal for data security. Queryable Encryption ensures that all data stored and retrieved from the MongoDB server remains encrypted until it is decrypted by the authorized MongoDB client. It aims to eliminate data exposure and attack surface on the MongoDB server or the Atlas SaaS service, while preserving operational transparency.

The company's Queryable Encryption is designed to bring two benefits: query preservation and query efficiency. Query preservation ensures that all current and previous queries are not altered. Existing queries and workflows can transparently take advantage of Queryable Encryption with no alteration. Query efficiency ensures that searches against encrypted data are still efficient.

In a traditional encryption scheme, a sensitive data field such as a name or social security number is often inefficient to decrypt. To simply query for a single item often means decrypting and sorting through all data records to correctly present the single item. As its name implies,Queryable Encryption efficiently answers the query to return the single item, without needing to decrypt all records within the same set.

Strategy

The company's strategy to position MongoDB as a "secure by default, secure by design" offering greatly simplifies its go-to-market message and reduces conflicts in selling, adoption and community. Historically, other data platform providers have sold security features as separately licensed add-ons.

These separate selling motions, sometimes with separately incentivized sales staff, can literally displace wallet share from core platform sales. Other times, security add-on sales are simply not worth the effort to pursue separately from the main data platform sale, so security sellers lose all possible account leverage that the core platform seller could bring.

MongoDB's strategy also reduces conflict within adoption among customers. Its security features are not externally mandated or separately managed side projects to the MongoDB implementation. Rather, the process of deploying security features is largely the same as deploying MongoDB.

Finally, MongoDB's strategy eliminates conflicts in the open-source community. Many vendors that are based on an open-source offering must choose what's best for the users against what's best for the vendor. By continuing to consistently apply features to all releases and distributions, MongoDB wants to avoid any fracturing or segmentation between different feature sets.

That said, MongoDB's Server Side Public License was created as a retort to major hyperscalers with their own managed MongoDB services. But the SSPL may also cause downstream SaaS providers that rely on MongoDB to be forced into purchasing a subscription, or to open-source the derivative work.

Competition

MongoDB's security approaches have several different competitors, yet given the product's strategy of secure by default, secure by design, perhaps it makes sense to look at how different competition weighs up against MongoDB as a whole. Hyperscalers such as AWS offer DocumentDB, and Azure offers CosmosDB. These releases indirectly compete with MongoDB Atlas, with limited support for MongoDB API compatibility.

As these offerings further diverge from MongoDB, the choice and gap between the hyperscalers' offerings versus MongoDB's only grows. Yet given broader themes of sovereignty, enterprises may be looking at how their data and their software enables confidentiality, authority and survivability. The appeal of the move to any platform is to eliminate short-term and long-term buyer's remorse – lowering the practical switching costs adds to the platform's attraction.

MongoDB will compete with traditional relational database offerings from Oracle Corp. and Microsoft Corp., as well as a host of PostgreSQL variants. But it also faces direct NoSQL competition from Couchbase Server, MarkLogic, ArangoDB, Redis Labs, DataStax and others with document model compatibility. There are notable feature differences between these offerings and MongoDB, including query composition and scaling for different workloads and applications.

Another level of MongoDB's competition may be the overall data security market. Many of these vendors advocate a neutral, broadly compatible platform for data governance, privacy or confidentiality, connecting to numerous different kinds of applications, workflows and business units. In an effort to appeal to all, data security may not be distinctive enough to any one particular application, workflow or business unit.

451 Research's recent Technology and Business Insight report on encryption in use identifies the particular challenge these nascent privacy-enhancing technologies have in struggling to find a problem their offering clearly and notably addresses. By building into an existing, broad platform such as MongoDB, Queryable Encryption may have greater traction and consumption than many other stand-alone data security offerings. Queryable Encryption and the earlier work of Kamara and Moataz have found a much more tangible serviceable market in MongoDB over a broader, yet more elusive, addressable market.

SWOT Analysis

STRENGTHS

MongoDB has been deployed by at least 35,000 customers, with many more using related Mongo API-compatible platforms. Based on open source, MongoDB builds its developer experience in the expectation that new MongoDB projects and adoption will continue to fuel growth.

WEAKNESSES

MongoDB must continue feature parity between all of its offerings. Fortunately, Queryable Encryption is available within all of its offerings, from the downloadable Community Edition to its enterprise Atlas offering. MongoDB arguably walks a delicate line with its SSPL and as software eats the world, more traditional enterprises may find themselves with a SaaS offering built with MongoDB.

OPPORTUNITIES

Data and software sovereignty may be a significant opportunity if MongoDB preserves feature parity between all of its offerings. Its secure by default, secure by design strategy greatly simplifies go-to-market, enabling security to be the icing on the MongoDB cake. Simplifying and clarifying this sovereignty by leading with its Atlas offering could be a significant influencer for MongoDB.

THREATS

MongoDB faces competition from hyperscalers, as well as relational database and NoSQL vendors. Developer choice in frameworks, languages and runtimes is incredibly diverse, with many combinations that could sidetrack or distract MongoDB's efforts to get more traction.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence