MongoDB Announces General Availability of End-To-End Data Encryption Technology

August 15, 2023

MongoDB Queryable Encryption enables organizations to meet the strictest data-privacy requirements by providing first-of-its-kind, end-to-end data encryption

CHICAGO, Aug. 15, 2023 /PRNewswire/ -- MongoDB, Inc. (NASDAQ: MDB), today at its developer conference MongoDB.local Chicago, announced the general availability of MongoDB Queryable Encryption, a first-of-its-kind technology that helps organizations protect sensitive data when it is queried and in-use on MongoDB. MongoDB Queryable Encryption significantly reduces the risk of data exposure for organizations and improves developer productivity by providing built-in encryption capabilities for highly sensitive application workflows—such as searching employee records, processing financial transactions, or analyzing medical records—with no cryptography expertise required. To get started with MongoDB Queryable Encryption, visit mongodb.com/products/capabilities/security/encryption.

"Protecting data is critical for every organization, especially as the volume of data being generated grows and the sophistication of modern applications is only increasing. Organizations also face the challenge of meeting a growing number of data privacy and customer data protection requirements," said Sahir Azam, Chief Product Officer at MongoDB. "Now, with MongoDB Queryable Encryption, customers can protect their data with state-of-the-art encryption and reduce operational risk—all while providing an easy-to-use capability developers can quickly build into applications to power experiences their end-users expect."

Data protection is the top priority among organizations across industries today as they face a growing number of regulations and compliance requirements to protect personally identifiable information (PII), personal health information (PHI), and other sensitive data. A common data protection capability organizations use to protect data is encryption, where sensitive information is made unreadable by cryptographic algorithms using an encryption key—and only made readable again using a decryption key customers securely manage. Data can be protected through encryption in-transit when traveling over networks, at-rest when stored, and in-use when it is being processed. However, working with encrypted data in-use poses significant challenges because it needs to be decrypted before it can be processed or analyzed. Organizations that work with highly sensitive data want to improve their security posture and meet compliance requirements by encrypting their data throughout its full lifecycle—including while it is being queried. Until now, the only way to keep information encrypted during the entire lifecycle was to employ highly specialized teams with extensive expertise in cryptography.

With the general availability of MongoDB Queryable Encryption, customers can now secure sensitive workloads for use cases in highly regulated or data sensitive industries like financial services, health care, government, and critical infrastructure services by encrypting data while it is being processed and in-use. Customers can quickly get started protecting data in-use by selecting the fields in MongoDB databases that contain sensitive data that need to be encrypted while in-use. For example, an authorized application end-user at a financial services company may need to query records using a customer's savings account number. When configured with MongoDB Queryable Encryption, the content of the query and the data in the savings account field will remain encrypted when traveling over the network, while it is stored in the database, and while the query processes the data to retrieve relevant information. After data is retrieved, it becomes visible only to an authorized application end user with a customer-controlled decryption key to help prevent inadvertent data exposure or exfiltration by malicious actors. With MongoDB Queryable Encryption, developers can now easily implement first-of-its-kind encryption technology to ensure their applications are operating with the highest levels of data protection and that sensitive information is never exposed while it is being processed—significantly reducing the risk of data exposure.

The MongoDB Cryptography Research Group developed the underlying encryption technology behind MongoDB Queryable Encryption, which is open source. Organizations can freely examine the cryptographic techniques and code behind the technology to help meet security and compliance requirements. MongoDB Queryable Encryption can be used with AWS Key Management Service, Microsoft Azure Key Vault, Google Cloud Key Management Service, and other services compliant with the key management interoperability protocol (KMIP) to manage cryptographic keys. The general availability of MongoDB Queryable Encryption includes support for equality queries, with additional query types (e.g., range, prefix, suffix, and substring) generally available in upcoming releases.

Since the release of MongoDB Queryable Encryption in preview last year, MongoDB has worked in partnership with customers including leading financial institutions and Fortune 500 companies in the healthcare, insurance, and automotive manufacturing industries to fine-tune the service for general availability.

Renault Group is at the forefront of a mobility that is reinventing itself. Strengthened by its alliance with Nissan and Mitsubishi Motors, and its unique expertise in electrification, Renault Group comprises four complementary brands—Renault, Dacia, Alpine, and Mobilize—offering sustainable and innovative mobility solutions to its customers. "MongoDB Queryable Encryption is significant for ensuring data protection and security compliance," said Xin Wang, Solutions Architect at Renault. "Our teams are eager for the architecture pattern validation of Queryable Encryption and are excited about its future evolution, particularly regarding performance optimization and batch operator support. We look forward to seeing how Queryable

Encryption will help meet security and compliance requirements."

About MongoDB
Headquartered in New York, MongoDB's mission is to empower innovators to create, transform, and disrupt industries by unleashing the power of software and data. Built by developers, for developers, our developer data platform is a database with an integrated set of related services that allow development teams to address the growing requirements for today's wide variety of modern applications, all in a unified and consistent user experience. MongoDB has tens of thousands of customers in over 100 countries. The MongoDB database platform has been downloaded hundreds of millions of times since 2007, and there have been millions of builders trained through MongoDB University courses. To learn more, visit mongodb.com.

Forward-looking Statements
This press release includes certain "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, or the Securities Act, and Section 21E of the Securities Exchange Act of 1934, as amended, including statements concerning MongoDB's technology and offerings. These forward-looking statements include, but are not limited to, plans, objectives, expectations and intentions and other statements contained in this press release that are not historical facts and statements identified by words such as "anticipate," "believe," "continue," "could," "estimate," "expect," "intend," "may," "plan," "project," "will," "would" or the negative or plural of these words or similar expressions or variations. These forward-looking statements reflect our current views about our plans, intentions, expectations, strategies and prospects, which are based on the information currently available to us and on assumptions we have made. Although we believe that our plans, intentions, expectations, strategies and prospects as reflected in or suggested by those forward-looking statements are reasonable, we can give no assurance that the plans, intentions, expectations or strategies will be attained or achieved. Furthermore, actual results may differ materially from those described in the forward-looking statements and are subject to a variety of assumptions, uncertainties, risks and factors that are beyond our control including, without limitation: the impact the COVID-19 pandemic may have on our business and on our customers and our potential customers; the effects of the ongoing military conflict between Russia and Ukraine on our business and future operating results; economic downturns and/or the effects of rising interest rates, inflation and volatility in the global economy and financial markets on our business and future operating results; our potential failure to meet publicly announced guidance or other expectations about our business and future operating results; our limited operating history; our history of losses; failure of our platform to satisfy customer demands; the effects of increased competition; our investments in new products and our ability to introduce new features, services or enhancements; our ability to effectively expand our sales and marketing organization; our ability to continue to build and maintain credibility with the developer community; our ability to add new customers or increase sales to our existing customers; our ability to maintain, protect, enforce and enhance our intellectual property; the growth and expansion of the market for database products and our ability to penetrate that market; our ability to integrate acquired businesses and technologies successfully or achieve the expected benefits of such acquisitions; our ability to maintain the security of our software and adequately address privacy concerns; our ability to manage our growth effectively and successfully recruit and retain additional highly-qualified personnel; and the price volatility of our common stock. These and other risks and uncertainties are more fully described in our filings with the Securities and Exchange Commission ("SEC"), including under the caption "Risk Factors" in our Quarterly Report on Form 10-Q for the quarter ended April 30, 2023, filed with the SEC on June 2, 2023 and other filings and reports that we may file from time to time with the SEC. Except as required by law, we undertake no duty or obligation to update any forward-looking statements contained in this release as a result of new information, future events, changes in expectations or otherwise.

Media Relations
MongoDB
press@mongodb.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/mongodb-announces-general-availability-of-end-to-end-data-encryption-technology-301901162.html

SOURCE MongoDB, Inc.