SOLUTION BRIEF

Gemalto SafeNet ProtectFile for MongoDB

Securing Sensitive Data in MongoDB Databases

MongoDB and Gemalto offer customers a simple, consolidated, and secure approach to the challenges posed to business in the era of Big Data.

Solution

Organizations are accumulating more data than ever. Sensors from the burgeoning Internet of Things, mobile applications with sensitive personal information, and websites delivering tailored advertisements, all send significant amounts of information to servers. The insights gleaned from this data drive operations and profits. Organizations need to be able to handle this data efficiently, at scale, and with the security to keep it safe. For many organizations, this data is their lifeblood and needs to be secured from risks (both internal and external) and for compliance reasons. Fortunately, MongoDB and Gemalto have a solution to meet these challenges.

MongoDB Enterprise Advanced

MongoDB is a cross-platform document-oriented database capable of incorporating any data type irrespective of where it comes from or what it looks like. Customers use MongoDB to consolidate disparate data types under a single view to gain real time perspectives on their data stores. Built-in scaling features and a flexible schema let the database grow automatically and transparently as customers collect increasing amounts of data of different types. Organizations are innovating by using MongoDB to create new types of applications, improve customer experience, and improve time to market all at increasingly lower costs.

SafeNet ProtectFile and SafeNet KeySecure

SafeNet ProtectFile seamlessly and transparently encrypts file data in MongoDB databases. Customers can use this transparent encryption to secure sensitive data (credit card numbers, personal information, logs, and more) that resides in flat files such as word processing documents, spreadsheets, images, designs, exports, archives, and backups. As MongoDB databases scale with increasing amounts of data, SafeNet ProtectFile is there every step of the way to secure data without hindering performance or the user experience.

SafeNet ProtectFile deploys in tandem with SafeNet KeySecure – a FIPS 140-2 Level 1, 2, or 3 validated hardware appliance for centralized encryption key and policy management. SafeNet KeySecure support for the Key Management Interoperability Protocol (KMIP) allows customers to centralize the management of SafeNet's encryption portfolio (in addition to SafeNet ProtectFile), as well as a broad ecosystem of other third-party encryption solutions.

Benefits

Transparent, Strong Encryption

- Apply transparent and automated encryption that secures data in MongoDB databases even as they scale

Apply granular access control policies

- Manage keys centrally in FIPS-certified key manager
- Prevent rogue root administrators from impersonating other users and accessing protected data

Secure Data Archival

- Keep data encrypted and inaccessible to administrators performing back-up and restore tasks

Secure Data Destruction

- Ensure all secured, sensitive data is rendered unreadable in the event destruction of data is required

Achieve Compliance

- Separate duties among administrators
- Track and audit access to protected data and keys
- Demonstrate full data control

Key Features

Separate Duties Among Administrators

The ability to separate duties based on business-need-to-know is an important security best practice. It ensures regulatory compliance and secures data from risks posed by privileged users. Both SafeNet ProtectFile and SafeNet KeySecure have granular access controls that decouple administrative duties from data and encryption key access. Administrators responsible for the management of the data center's physical infrastructure will be barred by access controls from viewing the data in the MongoDB databases that reside on the server being managed. Concurrently, SafeNet KeySecure administrators can only manage the security policies and keys on the key manager.

Improve Compliance

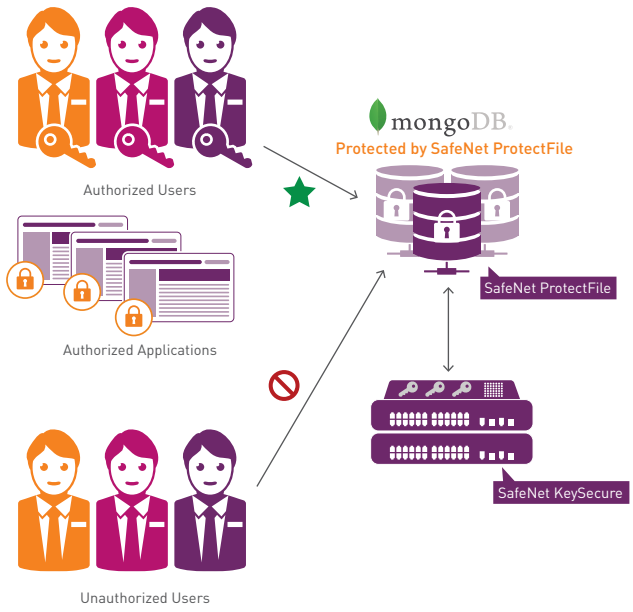
SafeNet ProtectFile helps achieve compliance with a variety of regulations that require encryption of data including, but not limited to, credit card numbers for Payment Card Industry Data Security Standard (PCI DSS) compliance, Personally Identifiable Information (PII) to comply with state data breach and data privacy laws, and Electronic Patient Health Information (EPHI) in accordance with HIPAA.

Simplified, Consoldiate Key Management

SafeNet KeySecure centralizes key administration behind an intuitive graphical user interface to make management easy. Additionally, its ability to consolidate keys, along with those used to secure MongoDB databases, from across the customer's infrastructure simplifies the organization's global encryption deployment. This simplified and consolidated approach to key management reduces risk by improving visibility and lessening the chance for error while also reducing the amount of time and investment needed to manage encryption throughout the organization.

Conclusion

The era of Big Data is here and organizations need to prepare for the rapid pace of innovation and analysis afforded by this additional data. The increase in opportunity comes with a distinct increase in the level of risk associated with that data. MongoDB and Gemalto offer organziations a joint solution to meet current and future needs in an efficient, agile and secure manner.
For more, visit: www.safenet-inc.com/Partners/MongoDB



About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry - leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free

© 2015 SafeNet, Inc. All rights reserved. SafeNet, the SafeNet Double Arrow logo, and other SafeNet trademark and service marks are the property of SafeNet, Inc. and/or SafeNet affiliated companies. SB (EN)-Oct.29.2015- Design: ELC