Implementing a Secure Big Data Environment

MongoDB and Vormetric

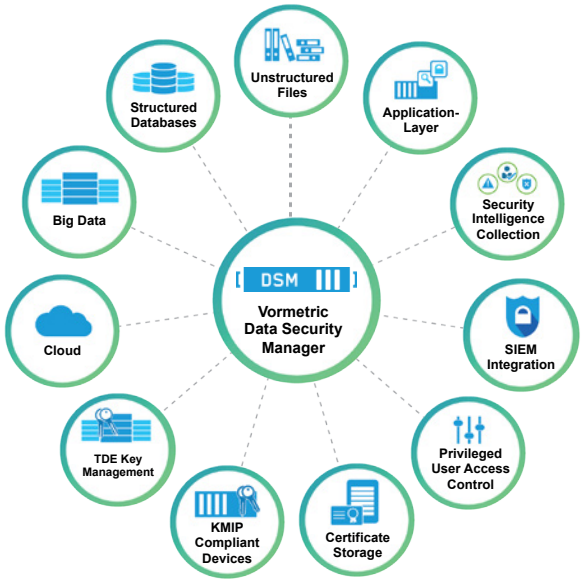
The evolution of Big Data is in high gear. It is an exciting time for marketers, scientists, analysts and others looking for competitive advantages and new discoveries by examining their data sources in new and unique ways. As organizations increasingly leverage Big Data, they are looking at ever-larger data sets across files and databases, as well as building on their previous Big Data results. These strategic and aggressive efforts to draw enhanced insight out of a growing number of data sets commonly involve sensitive or regulated information.

MongoDB is the leading next generation database, empowering businesses to be more agile and scalable. Found in more than 1/3rd of Fortune 100 companies and startups alike, MongoDB is being used to create new classes of applications, improve customer experience, accelerate time to market and reduce costs. With its dynamic schema, MongoDB is made to store, manage, and analyze rapidly changing structured, semi-structured, and unstructured data. MongoDB was designed to ensure data security and offers a host of protection technologies including robust authentication, role-based access control, encrypted communications, and strong auditing capabilities.

However, it is also critical to protect data-at-rest against privileged users who have no need to access the data and attacks that bypass the database and target the underlying servers or physical storage. This data-at-rest includes the collection of unstructured files and structured databases, query reports, log files and other data sets that might contain sensitive or regulated information spread and copied across the infrastructure.

The Vormetric Data Security Platform

Vormetric, a MongoDB Advanced Partner, compliments MongoDB security by delivering high-performance encryption, easy to use integrated key management, privileged user access control, and generates data access security intelligence with the Vormetric Data Security Platform. Unlike other solutions, this extensible platform is tunable to protect data as granular as specific columns within a relational database or fields within a document in MongoDB, or it can protect all the data within a given directory or volume. The platform supports the broadest range of operating systems and environments in the industry, delivers operations efficiencies through high-performance and centralized management with the Vormetric Data Security Manager (DSM).



The Vormetric Data Security Manager centralizes and simplifies organization-wide data-at-rest security and control

mongoDB

"Organizations have pushed vast amounts of data into these big data clusters, but most have implemented virtually zero security measures."

"Securing Big Data: Security Recommendations for Hadoop and NoSQL Environments." Securosis - October 2012

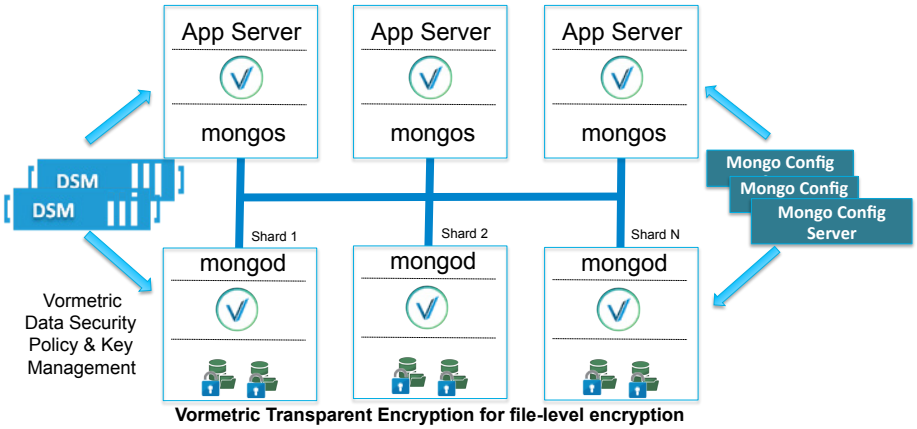
"Vormetric Data Security Platform is useful in big-data scenarios, since it is relatively straightforward to work with both structured databases and unstructured files that are often combined in a big-data exercise. Vormetric can encrypt the initial data as well as the results of a big-data run, which are often more valuable than the initial data."

- Garrett Bekker, 451 Research, March 2014

The Vormetric Data Security Platform with MongoDB

- Encryption, centralized key management, privileged user access control and security intelligence logs for data-at-rest across the MongoDB environment: ingress data, egress reports, as well as configuration files and audit logs.
- Transparently protect new and complex structured and unstructured data types without application engineering with Vormetric Transparent Encryption.
- Simplify adding document-level encryption with tools that include sample code and API support (Java and C/C++) for MongoDB application integration with Vormetric Application Encryption.
- Generate security intelligence on data access by users, processes and applications accessing data anywhere across the MongoDB infrastructure.
- Maintain SLAs with high-performance encryption and high-availability data security architecture.

Vormetric Application Encryption for field and column-level encryption



Vormetric Transparent Encryption for file-level encryption

The Vormetric Data Security Platform can secure data at the application server, shard, or a combination of both.

Example Customer Use Cases

A Leading healthcare organization, launched a service powered by MongoDB and made use of Private Health Information (PHI), requiring them to adhere to HIPAA/HITECH regulations. The combination of MongoDB and Vormetric enabled the company to deploy their service with the required performance and security level.

A Fortune 500 industrial manufacturer was required to collect sensitive and valuable data from systems in the field and provide that data to regulatory agencies. MongoDB with Vormetric was selected by IT and approved by the agency auditors to handle this large data set, in a compliant manner, without disrupting the existing SLAs.

About MongoDB

MongoDB makes development simple and beautiful. For tens of thousands of organizations, MongoDB provides agility and the freedom to scale. Fortune 500 enterprises, startups, hospitals, governments, and organizations of all kinds use MongoDB because it is the best database for modern applications. Through simplicity, MongoDB changes what it means to build. Through openness, MongoDB elevates what it means to work with a software company. Please visit www.MongoDB.com to learn more.

About Vormetric

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1300 customers, including 17 of the Fortune 25 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters — their sensitive data — from both internal and external threats. For more information, please visit: www.vormetric.com.

Supports Compliance

PCI, HIPAA, European Commission, NIST, FedRAMP, FISMA

Key Capabilities

- Data-at-Rest Encryption
- Privileged User Access Control
- Security Intelligence Collection
- High-performance
- Ingress and Egress Protection
- Field to File-level Encryption
- Centralized Policy and Key Management

Deployment

- Application-layer encryption at App Server
- File-system level encryption across infrastructure
- Flexible environment support: Cloud, Big Data, Enterprise Data Center
- DSM available as physical or virtual appliance

Vormetric, Inc.
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
South Korea: +82.2.2190.3830
info@vormetric.com
www.vormetric.com