Securing Sensitive Data in Cassandra NoSQL Databases
Using the SafeNet Data Protection portfolio for scalable security in distributed environments

Gemalto and Apache meet organizations’ big data needs with a secure, scalable, and cost-effective NoSQL database solution.

The massive volumes of data from sensors, clicks, and purchases that organizations are collecting need to be organized for analysis so they can be mined for insights that better decision making and improve performance. Apache Cassandra is a new breed of database – called NoSQL – that can handle these data volumes efficiently, reliably, and cost-effectively all at enterprise scale. However, these data volumes contain significant amounts of sensitive data that needs to be secured for organizations to be safe and compliant. Fortunately, Gemalto offers solutions to meet these challenges.

Apache Cassandra
Apache Cassandra is an open-source database designed to handle large volumes of data by distributing it across large collections of commodity servers – both on-premises and in the cloud. Data is replicated across Cassandra nodes to ensure reliable data availability. This decentralization makes scaling easy with performance and capacity responding linearly. Organizations using Cassandra deploy and use only the resources they need without the excess capacity or cost of large mainframes.

SafeNet Data Protection Portfolio
Gemalto’s SafeNet data protection portfolio secures data anywhere in its flow from creation to storage. Each solution deploys with SafeNet KeySecure, a FIPS validated appliance for centralized key and policy management. In addition to SafeNet keys, SafeNet KeySecure manages keys for Cassandra’s transparent data encryption (TDE). The following solutions can be used to secure Cassandra NoSQL databases.

SafeNet ProtectFile
SafeNet ProtectFile is a file-level encryption solution that seamlessly and transparently protects sensitive file data in Cassandra NoSQL databases, such as credit card numbers, personal information, logs, and more.

Benefits

- **Transparent, Strong Encryption**
  - Apply transparent automated encryption that secures Cassandra database data even as new nodes are added
- **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
- **Automatic Protection**
  - As data is replicated across nodes it is automatically encrypted so that it is secure wherever it goes
- **Keeps Cassandra Secure in the Cloud**
  - SafeNet solutions are cloud agnostic meaning they work in any cloud enabled environment
- **Achieve Compliance**
  - Track and audit access to protected data and keys
  - Demonstrate full data control

SafeNet ProtectApp
SafeNet ProtectApp is an API based application-level encryption solution that lets customers incorporate protection directly into their apps to secure both structured and unstructured data as it is generated before it is stored in a Cassandra database.

SafeNet Tokenization
SafeNet Tokenization protects high value information in databases by replacing it with a surrogate value or “token” without changing the database table or the file layout. Systems protected with tokenization are removed from the scope of certain regulations such as PCI DSS.
**SafeNet ProtectV**

SafeNet ProtectV is a full disk encryption solution for virtual machines running Cassandra nodes. SafeNet ProtectV extends its protection to associated storage volumes, instance snapshots, backups, and partitions so security teams can maintain ownership and control of their data and encryption keys at all times.

**Key Features**

**Duty Separation Among Administrators**

Separating administrative duties is an important best practice that ensures compliance and protects data from risks posed by privileged users. The SafeNet data protection portfolio includes policy-based access controls that separate database administrative duties from data and encryption key access. Database administrators will be prevented from viewing the data in Cassandra databases. Concurrently, SafeNet KeySecure administrators manage only the security policies and keys on the key manager without ever seeing protected data.

**Achieve Compliance**

The SafeNet data protection portfolio helps organizations achieve compliance with 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, Consolidated Key Management**

SafeNet KeySecure centralizes key administration behind an intuitive graphical user interface to make management easy. It supports the Key Management Interoperability Protocol (KMIP) so customers can also consolidate and centrally manage keys from a broad ecosystem of partners — including Cassandra TDE. Simplified, consolidated management mitigates risk by improving visibility and lessening the chance for error while also reducing the time and investment needed to manage encryption throughout the organization.

**Automated Scalable Security**

Cassandra’s ability to automatically replicate data across nodes to ensure availability is a key part of its value. SafeNet solutions integrate to ensure that data is encrypted – at the file system-, application-, or volume-level – as it replicates to each node. Additionally, SafeNet encryption is cloud agnostic and works in any cloud-enabled environment making Cassandra equally secure in the cloud as it is on-premises. SafeNet KeySecure’s key management simplifies large scale administration to make large scale deployments easy to manage.

**Conclusion**

The era of big data will continue to rapidly produce data that will need to be organized in order to be made useful for analysis and eventually innovation. The new opportunities aren’t without risk. While Cassandra can organize that data, Gemalto will be there to offer protection in an efficient, and scalable manner. For more, visit: [http://www.safenet-inc.com/Partners/Cassandra/](http://www.safenet-inc.com/Partners/Cassandra/)

**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 safenet.gemalto.com

**Follow Us**: blog.gemalto.com/security

©Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, the Gemalto SafeNet logo, and are trademarks and service marks of Gemalto and are registered in certain countries. SB (EN) - Sept 20, 2016 - Design: FR