Fortanix®

Leader in Confidential Computing

Solution Brief

MariaDB Database Encryption with Fortanix DSM

The Need

Providing transparent data encryption at scale, with high usability and low TCO has been a challenge with legacy databases, and still remains a challenge with the new modern databases. Reason being: Key management and HSM solutions were not designed to meet the scale and performance of large-scale deployments of databases. And they did not change or evolve in many years.

The frustrating bottom line is that the number of databases and the volumes of data grow at a much faster pace than the innovation in data encryption.

Until today.

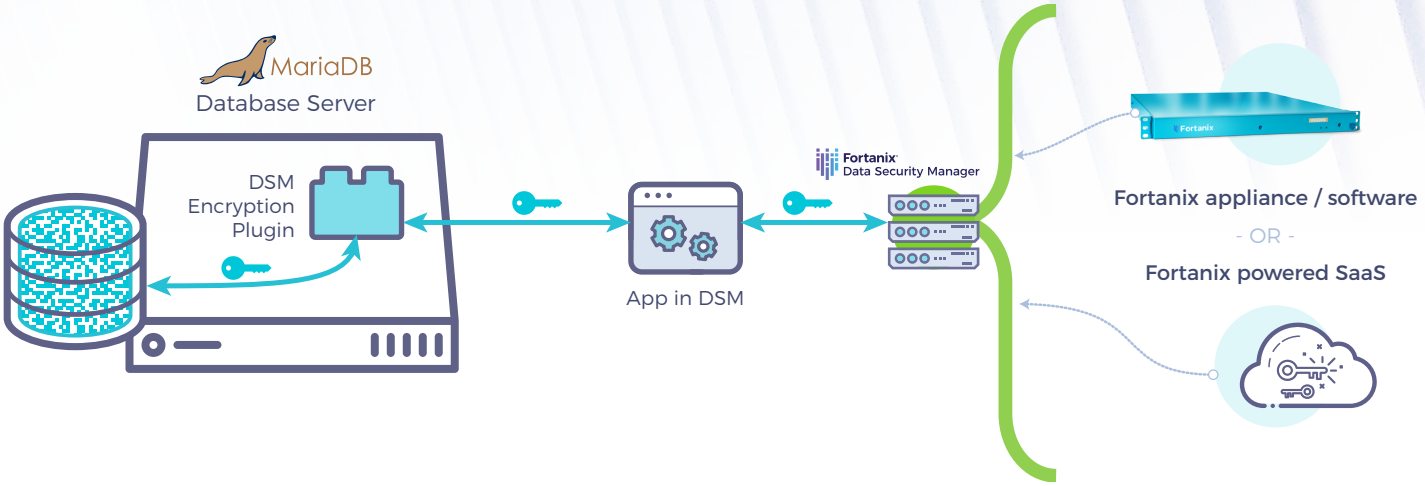
Enter Fortanix DSM.

MariaDB

Fortanix Data Security Manager™ (DSM), was designed to meet these exact requirements: Scale, performance, breadth and depth of features, and most of all – operational flexibility. Incorporating key management, HSM, tokenization and secrets management in one enterprise encryption platform, DSM can run in the cloud, on-premises, in hybrid environments and can also be delivered as SaaS and managed service.
DSM leverages Intel SGX® processors to securely store the keys inside HSM, making it the most secure encryption solution for any database.

Presently, DSM is the only solution backed by hardware for encryption of data-at-rest in MariaDB.

info@fortanix.com | +1 (628) 400 2043 | 444 Castro St #305 Mountain View, CA 94041



Fortanix DSM for MariaDB database encryption

Following MariaDB's best practices, Fortanix created a plugin that integrates with DSM to generate and manage the AES keys required to encrypt the data on MariaDB. The plugin generates and manages the encryption keys and carries out the actual encryption and decryption of the data. It seamlessly supports the use of multiple encryption keys, which are are stored securely in DSM, with hardware-level encryption. To encrypt new data or decrypt existing data in the database, the database, the key meta-data is used to fetch the key from DSM when needed, assuring the keys are never exposed when not in use.

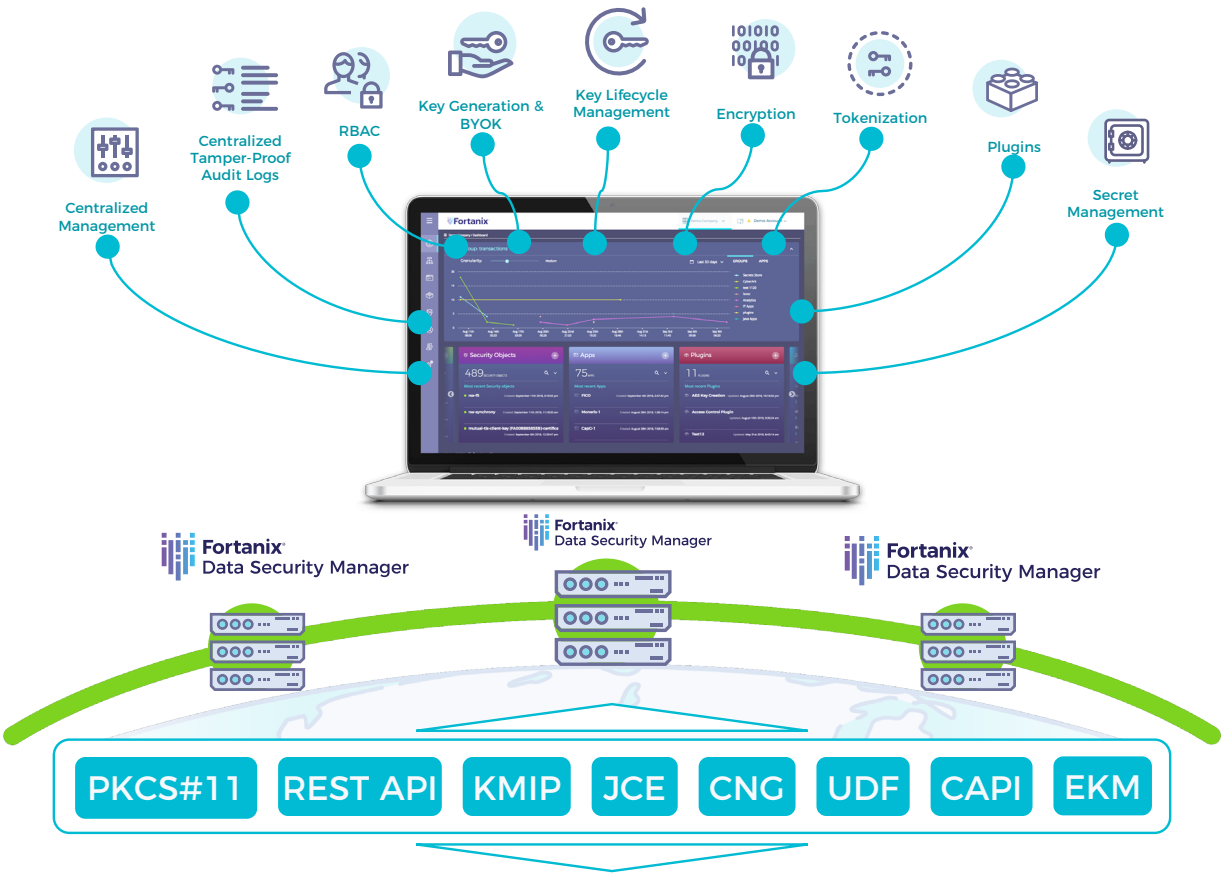
For technical details and user-guide about Data-at-Rest encryption in MariaDB using Fortanix DSM , please visit https://support.fortanix.com/hc/en-us/articles/360028282032-Using-DSM-for-MariaDB-Encryption-at-Rest

Benefits

- **Single Solution:** Unified key management, HSM, tokenization and secrets management
- **Security:** HSM security. No key material resides on the database server. Secure lockdown of the entire database when needed.
- **Scalability:** DSM can easily scale to provide encryption to tens of thousands of MariaDB instances in any number of locations, centrally managed at all times.
- **Ease of use:** Workflow-based via Web GUI and REST API-based for programmatic operations.
- **Fined Grained Control:** Selective disabling/enabling of keys through the UI to lock the database.
- **Key Lifecycle Management:** Including seamless support of key rotation and versioning.
- **Audit Logs:** Tamper-proof audit logs capture every operation and are easily integrated with SIEM.

About Fortanix Data Security Manager (DSM)

- The next-generation cryptographic services platform, offering key generation, management, distribution, encryption-as-a-service, secrets management, tokenization and HSM — all delivered as a single product.
- Available in multiple deployment modes: SaaS, dedicated-tenant, managed tenant and self-hosted service.
- DSM' SGX hardware is FIPS 140-2 level 3 certified.
- Offers simple central management, server-side load balancing, central tamper-proof logging, RESTful APIs, Confidential Computing plugin to run custom code and wide integration with leading public clouds, databases, and other solutions.



{ Easy integration with SIEM, AD, PAM }

[Fortanix DSM Datasheet]

[Fortanix DSM Appliance]