



# Fortanix Data Security Manager for VMware Sovereign Cloud

## Market need

VMware Sovereign clouds offer continuous protection and secure accessibility controls to enable new values and opportunities data protection. Protect and control confidential or restricted data with the data residency and data sovereignty that a sovereign cloud provides, ensuring compliance with changing data privacy laws using a trusted cloud that supports a nation's digital economy. Virtual environments running VMware can readily leverage vSphere VM Encryption or vSAN encryption to protect VMs and data-at-rest. However, enterprise key management that is both secure and adaptable to a dynamic software-defined infrastructure remains a challenge. Traditional HSMs require proprietary hardware and are inflexible for a software-defined data center. Software-only key managers on the other hand do not offer the protection of HSMs.

## Solution Overview

The joint VMware and Fortanix solution offer scalable data protection and compliance for VMware Sovereign cloud environments. Fortanix Data Security Manager (DSM), is a unified HSM and Key Management solution that easily integrates via KMIP for VMware vSAN and vSphere VM encryption, enabling sovereign cloud customers to bring and manage their own keys. Fortanix DSM makes it possible for VMware Sovereign cloud providers to deliver Data Protection and compliance to the end customers (tenants). Secured with Intel® SGX, Fortanix DSM delivers HSM security with software defined simplicity, and a cloud scale architecture.

Fortanix DSM with built-in multi-tenancy, when integrated together with VMware Sovereign cloud, enables service provider partners the ability to offer Bring Your Own Key (BYOK) for VM encryption and vSAN Encryption, FIPS 140-2 Level 3 HSM protection, key management, tokenization, and secrets management through a single platform, hosted within the VMware Sovereign Cloud boundary.



## Joint Use Cases



### Bring your own key for VM and vSAN encryption

Fortanix Data security provides VMware users an option to bring their own keys to encrypt VMs/vSAN and other encryption use cases



### Complete Key lifecycle Management

Fortanix delivers full key lifecycle management as a service to ensure secure and consistent key management across on-premises and multicloud environments, including bring your own key (BYOK) and bring your own key management service (BYOKMS).



### FIPS 140-2 Level 3 HSM backed platform

Customers store the keys in the Fortanix FIPS 140-2 Level 3 certified HSM and cryptographic operations are executed securely within the hardware.



### Tokenizing Sensitive Data

Combination of Format Preserving Tokenization (FPE) and role-based access control (RBAC) for application running on VMware Sovereign, helps in protecting sensitive data. With Fortanix, relevant users can get authenticated through RBAC, query the data, and tokenize data on the fly.



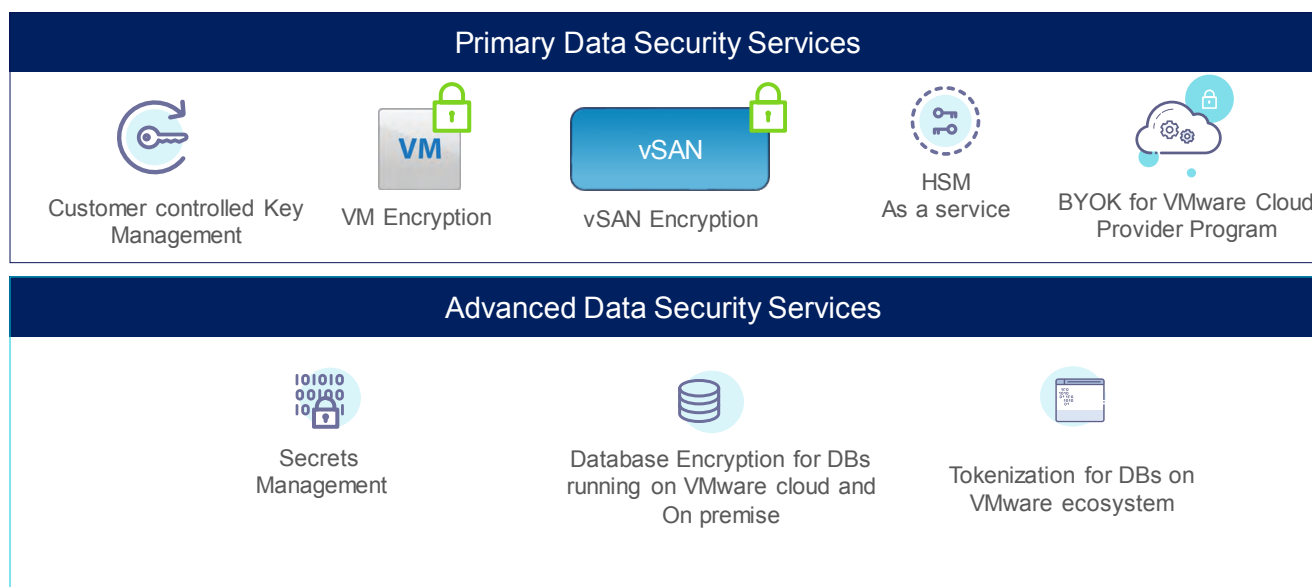
### Database Encryption

Fortanix integrates with native database encryption to manage and store the cryptographic keys required to encrypt all your databases including Oracle, SQL Server, MongoDB, Postgres, MySQL, Maria DB, IBM DB2 and more on VMware Sovereign cloud.



### Secrets Management

Fortanix offers a secure secrets management solution that can manage secrets natively in the cloud and on-premises, providing extensive RESTful APIs through open standards such as OAuth, OpenID (SAML), LDAP, JWT, and PKI.





## Benefits of using Fortanix Data Security Manager in VMware Sovereign Clouds



### QUICK TIME TO VALUE

5 Minutes for implementation versus 2-3 weeks with other HSM services



### GREATER CONTROL OVER THE KEYS

Control the keys externally, turn the keys off, turn them on when required and get control over data



### OWN YOUR DATA AND KEYS

Using Fortanix DSM, VM encryption keys for are managed and owned by the customers



### STRICT ACCESS CONTROL AND QUORUM APPROVALS SAFEGUARD DATA

Segregation of the key management operations based on roles and permissions ensures control over data



### MEET GDPR AND SCHREMS II REGULATIONS

FIPS certified HSM and key management with regional level isolation helps meet specific data privacy regulations.

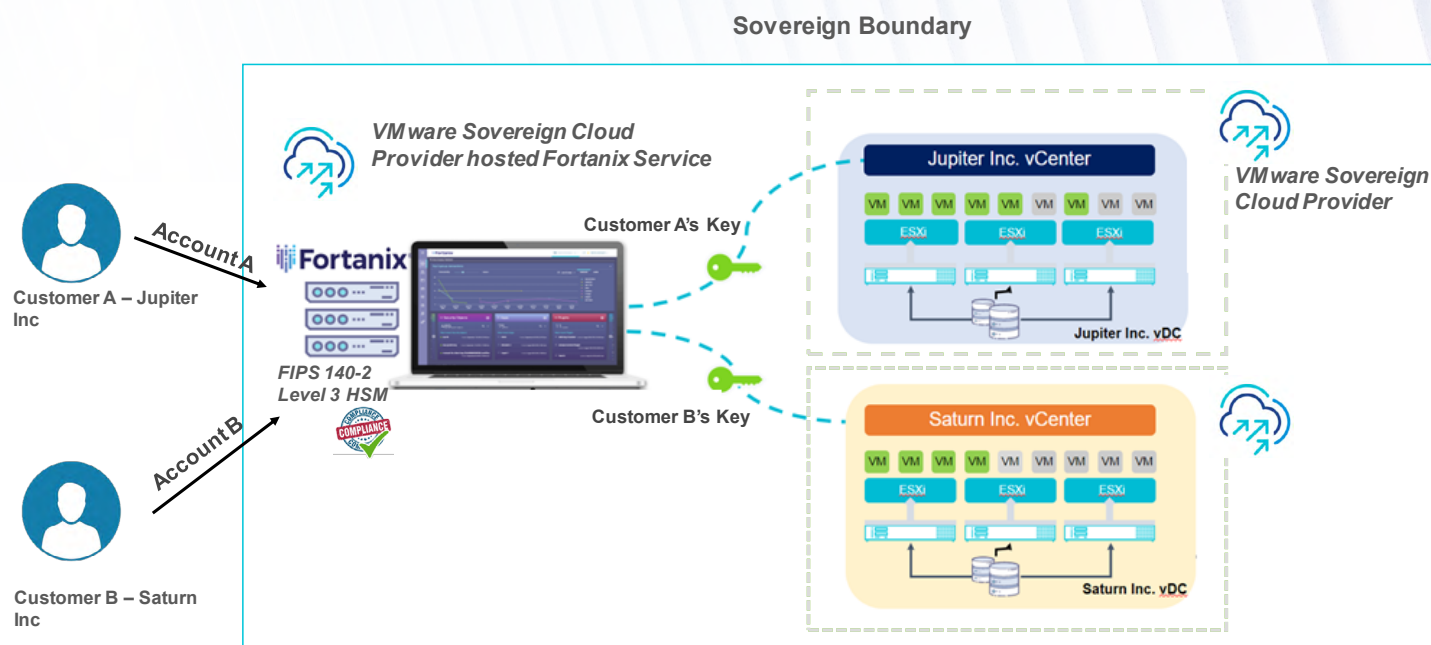
## Deployment – VMware Sovereign cloud Boundary

The VMware Cloud Provider partners can host Fortanix Data Security Manager out of the HSM appliances running in their data centers within the VMware Sovereign cloud boundary. Each VMware Sovereign cloud customer will have a dedicated vCentre where they can configure Fortanix Data Security Manager as an external key manager. The customer will have full control of the keys and the VMware Cloud Provider partner will have zero access/visibility to the keys. The keys never leave the sovereign cloud boundary.

- **Only Customers will have access to the keys. Providers have zero visibility.**
- **Keys will be generated and managed in Customer controlled Fortanix DSM account**
- **Multi-tenancy- Each customer account is separated from each other**



## Fortanix DSM for VMware Sovereign Cloud: Multitenancy Platform with Customer managed keys



### About Fortanix

Fortanix® is the data-first multicloud security company. As the industry's first and largest provider of confidential computing solutions, Fortanix decouples data security from infrastructure. Fortanix solutions empower organizations with centralized controls to secure data spread across clouds, applications, SaaS, databases, and data centers. Over a hundred enterprises worldwide, especially in privacy-sensitive industries like healthcare, fintech, financial services, government, and retail, trust Fortanix for cloud security and privacy. Fortanix investors include Intel Capital, Foundation Capital, Neotribe Ventures, and In-Q-Tel. Fortanix is headquartered in Mountain View.



Learn more at

[www.fortanix.com/vcpp/](http://www.fortanix.com/vcpp/)

### About VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with VMware Cross-Cloud Architecture™ and solutions for the data center, mobility, and security.



Learn more at

[www.vmware.com/cloud-solutions/sovereign-cloud.html](http://www.vmware.com/cloud-solutions/sovereign-cloud.html)

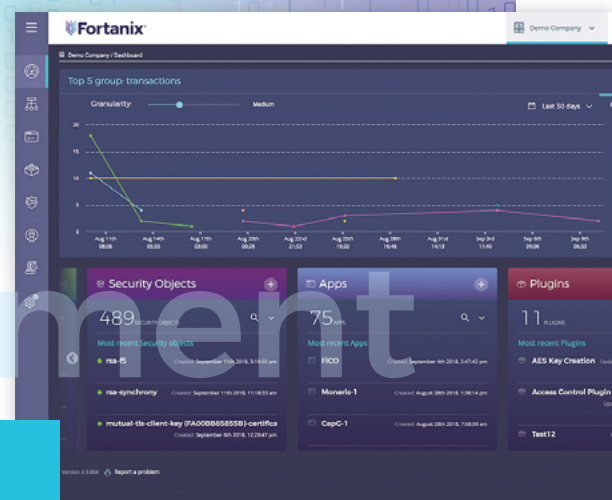




DATA SHEET

# Fortanix Data Security Manager (DSM)

## Next generation HSM and Key Management



As you shift your applications to new infrastructures, you need a solution that can protect all your data on-premises as well as in the cloud. Fortanix Data Security Manager delivers HSM, Key Management, Encryption, and Tokenization for your hybrid and cloud-native applications, all from the same integrated solution. Fortanix introduces a radical new technology — Runtime Encryption, and a new product architecture. With Fortanix Data Security Manager, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data<sup>1</sup>.



### UNIFIED PLATFORM

Fortanix Data Security Manager (DSM) is a unified platform for data security that combines encryption, key management, tokenization, and secret management in a single solution.



### CLOUD AND DEVOPS FRIENDLY

KMS supports extensive RESTful APIs, PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG. Easily support all existing and new applications, whether operating in public, private, or hybrid cloud.



### SIMPLIFY OPERATIONS

Fortanix provides a “single pane of glass” modern, multi-tenant, and intuitive user interface for simplified administration and increased control, including extensive logging and auditing across your entire infrastructure.

## Key Features and Benefits

- UNIFIED DATA PROTECTION:** Integrated HSM, KMS, Secrets Management, Encryption and Tokenization functionality. Support for full NSA Suite B algorithms: RSA, AES, Elliptical Curve<sup>2,1</sup>. Perform broad cryptographic operations and key management operations, including key generation, key import, key rotation, key derivation, encryption, decryption, signing, verification, tokenization, and masking
- COMPLETE PRIVACY:** End-to-end security for keys and data (at-rest, in-transit, and in-use) protected with layers of defense including Fortanix Runtime Encryption®, Intel® SGX and FIPS-validated hardware; Only authorized users can access keys
- CENTRALIZED VISIBILITY AND CONTROL:** Centralized intuitive web-based user interface for management. Role-based access control (RBAC) for users, applications and groups with segregation of duties. Comprehensive tamper-proof audit logs to track all activity, including administration, authentication, access, and key operations
- APPLICATION FRIENDLY INTERFACES:** Support for RESTful APIs, PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG. Easily support all existing and new applications, whether operating in public, private, or hybrid cloud.



- **ADVANCED ADMINISTRATION:** Single Sign-on support (SAML, OAuth, and Active Directory/LDAP). Auditing integration with SIEM tools (Syslog, Splunk, and CSP logging). Quorum approval policy (M of N) for enhanced protection
- **RUNTIME ENCRYPTION PLUGINS:** Securely run sensitive business logic inside trusted boundary with Runtime Encryption plugins. Easily create or customize cryptography logic for your unique business or security requirements
- **CLOUD-SCALE PROTECTION:** Distributed scale-out architecture provides scalable performance on demand. Simplified operations with built-in synchronization, high availability and disaster recovery
- **INTEGRATE AND MANAGE KEYS IN LEGACY AND CLOUD HSMS:** HSM gateway, an extended capability of Fortanix Data Security Manager manages keys in legacy and cloud HSMS and helps consolidate HSM infrastructure.
- **FLEXIBLE DEPLOYMENT OPTIONS:** Fortanix offers flexible deployment options like Software, SaaS, Hybrid, VMWare and FIPS 140-2 level 3 certified appliance.
- **FLEXIBLE LICENSING:** Organizations have the option to purchase the base package, and depending on the use cases add more capabilities.

- **FLEXIBLE CONSUMPTION:** Designed to run in and support all environments: on-premises environment, private cloud, edge cloud, public cloud, managed environments. Flexible consumption options: either a FIPS validated appliance, software on SGX-enabled servers/laaS or SaaS providing you a ubiquitous solution for your multi-cloud applications



## Deployment Architecture

Fortanix Data Security Manager delivers quick time to value — new nodes can be deployed and provisioned without requiring any initial configuration in a centralized place. Once deployed, a Fortanix DSM cluster can be managed and monitored remotely and without need for physical access.

