

# Fortanix Self-Defending Key Management Service™

## 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 Self-Defending KMS™ 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 Self-Defending KMS, 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>.



### INSTANT VALUE

Quick time to value with rapid deployment, simplified operations and centralized management



### SCALE ON-DEMAND

Scale as you need to support millions of clients and billions of transactions with auto-mated load-balancing and high availability

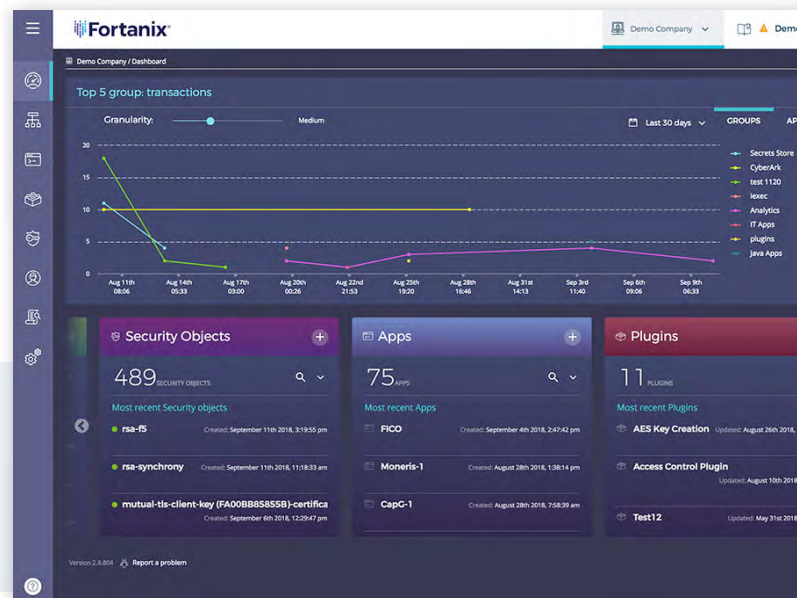


### LOWER TCO

Transparent, simple, and predictable pricing. No additional costs for clients, connectors, features or algorithms

## Key Features and Benefits

- UNIFIED DATA PROTECTION:** Integrated HSM, KMS, 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



1. Tokenization and secrets management are offered at an additional charge.

2 See algorithms supported here -

<https://support.fortanix.com/hc/en-us/articles/360016160411-Algorithm-Support>

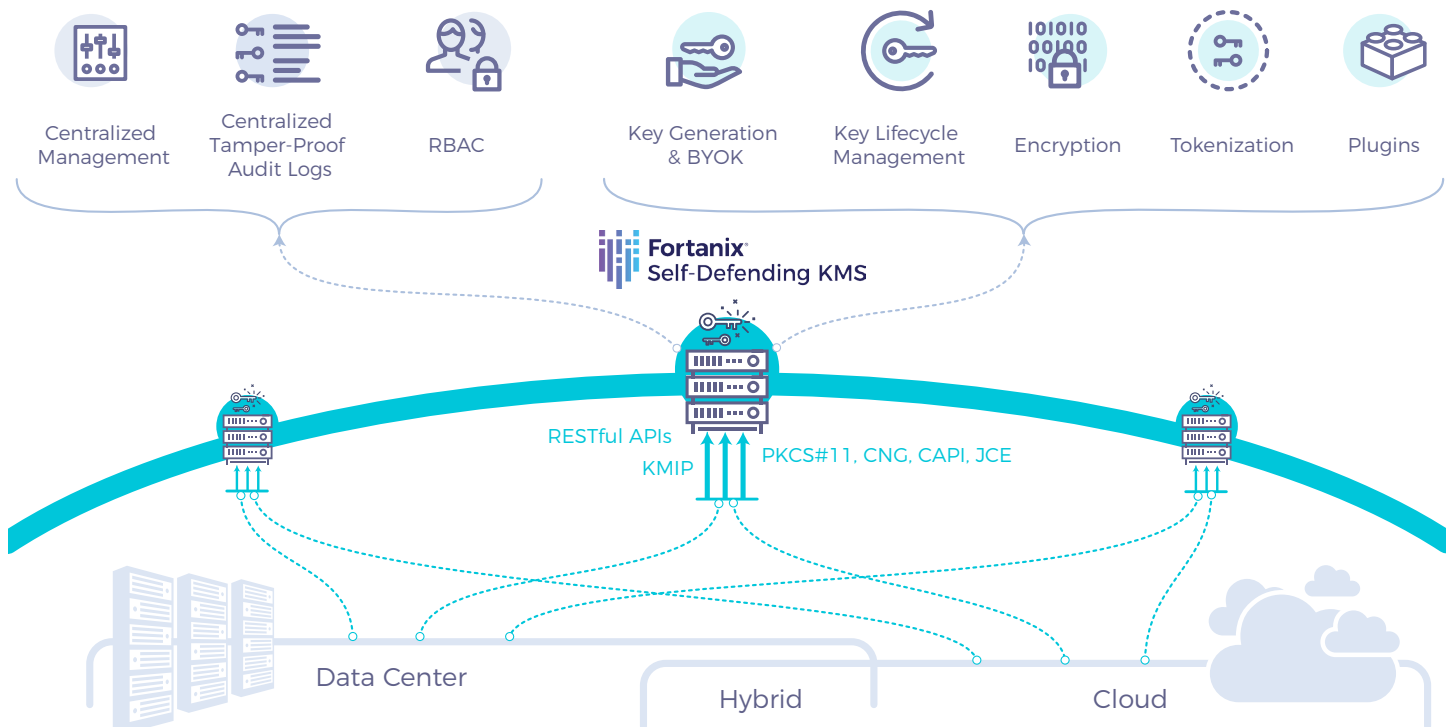


- **APPLICATION FRIENDLY INTERFACES:** Support for RESTful APIs, PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG. Easily support all existing and new applications, whether operating in public, private, or hybrid cloud. Out of the box connectors with no additional license costs
- **ADVANCED ADMINISTRATION:** 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

- **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

Fortinix Self-Defending KMS delivers quick time to value — new nodes can be deployed and provisioned without requiring any initial configuration in a centralized place. Once deployed, a Fortinix Self-Defending KMS cluster can be managed and monitored remotely and without need for physical access.



# Use Cases



## SECURE CLOUD ADOPTION

Make a secure and seamless transition to hybrid or multi-cloud. With a scalable distributed architecture and easy to use BYOK support for major cloud providers, Fortanix Self-Defending KMS can service encryption for any application in any cloud.



## DATA AT REST ENCRYPTION

Address performance and availability requirements for the encryption of distributed databases, data lakes, or storage systems with scalable distributed key storage with auto synchronization capabilities of Fortanix Self-Defending KMS.



## SECURE VIRTUAL ENVIRONMENTS

Accelerate data protection and compliance for virtualized environments with enterprise-wide key management and KMIP-based integration for native encryption solutions.



## PKI / IOT SECURITY

Enable secure remote manufacturing with Fortanix Self-Defending KMS. The solution helps establish chain of trust from birth of the device throughout the entire lifecycle.



## NETWORK SECURITY (TLS TERMINATION)

Close the encryption gap with the ability to keep all the keys in the trust boundary with Fortanix Self-Defending KMS.



## BLOCKCHAIN KEY MANAGEMENT

Blockchain Key Management: Fortanix Self-Defending KMS delivers unmatched security and availability for Blockchain private keys including support for powerful yet easy to use policies for multi-sig with quorum approval, and strong access control



## REGULATORY COMPLIANCE


Cost-effectively achieve compliance for GDPR, PCI-DSS, and data privacy laws with fine-grained access control and comprehensive auditing



## SECURE CODE / BUSINESS LOGIC

Easily implement new cryptographic algorithms, unique key derivation, or advanced access control policies using Runtime Encryption Plugins. Run inside the secure boundary of Fortanix Self-Defending KMS.

# Fortanix vs. Traditional HSM/KMS Solutions

Feature/Attribute	 	Traditional HSM/KMS
1. Consumption options	<b>Flexible options: software on servers, Appliance, SaaS</b>	Proprietary hardware
2. Total cost of ownership	<b>Predictable all-inclusive model, no additional costs for connectors</b>	Needs specialized expertise required to maintain, complicated pricing based on multiple variables
3. Security	<b>FIPS 140-2 pending, security extends to KMS, authentication, authorization</b>	FIPS 140-2, security limited to keys and key operations
4. Horizontal scalability	<b>Infinitely scalable</b>	Not scalable
5. Storage capacity	<b>Increases linearly with size of cluster</b>	Very limited
6. Performance	<b>Single node 25% faster than fastest HSM, and then increases linearly with size of cluster</b>	Limited based on hardware configuration
7. High availability	<b>Built-in redundancy and fault tolerance in cluster</b>	Generally achieved by replicating HSMs, done using client's help
8. Seamless disaster recovery and backup	<b>Built-in</b>	Not available
9. Multi-region support	<b>Single cluster can span multiple continents</b>	Not available
10. Multi-user support	<b>Integrates with single-sign on, authorization using RBAC, advanced quorum control</b>	Not available
11. Multi-app and multi-client support	<b>Strong separation of key space across clients and apps</b>	Key space shared across clients and apps
12. Secure code execution	<b>Run sensitive business logic with easy to develop and use Runtime Encryption plugins</b>	Limited support to run code written using proprietary SDK in constrained environments, often requires professional services
13. Supported data types	<b>No limitations on nature of stored data (keys, data, applications, etc.)</b>	Can only store keys & related security credentials
14. Audit logs	<b>Secure, comprehensive, tamper proof</b>	No audit logs for key operations, some support for getting appliance health information
15. KMIP	<b>First solution to provide HSM and KMIP in a single product</b>	Sold as separate appliances
16. Tokenization	<b>Support for many common fields including SSN, DOB, PAN, and more</b>	Sold as separate appliances or products