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.

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. 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, ICE, 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.1

---

1. Tokenization and secrets management are offered at an additional charge.
• **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/IaaS or SaaS providing you a ubiquitous solution for your multi-cloud applications

---

**Deployment Architecture**

Fortanix 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 Fortanix Self-Defending KMS cluster can be managed and monitored remotely and without need for physical access.