

Application-level Encryption

Problem

More and more apps are operating on private data. And most of the developers don't have the time or expertise to implement data privacy and security. Encryption is the only way developers can keep their apps secure. Developers also need to add in additional layers of security. They need to think about how the app data is being accessed and provide strong authentication controls.

Solution Overview

Fortanix offers a comprehensive Data Security as a Service (DSaaS) platform that provides integrated hardware security module (HSM), key management, encryption and tokenization capabilities. Using APIs, developers can easily integrate encryption, data access control and key management into the application. Rest APIs can also be used to tokenize sensitive data.

Solution Benefits



INTEGRATED DATA SECURITY PLATFORM

Fortanix provides a Data Security as a Service (DSaaS) platform with integrated hardware security module (HSM), key management, encryption and tokenization capabilities.



EFFECTIVE POLICY MANAGEMENT WITH ROLE-BASED ACCESS

Fortanix provides policy-based app level encryption with selective access based on segregation of users and roles providing security and privacy of data, while also enabling compliance with regulations, such as, PCI-DSS, GDPR.



SUPPORT FOR APIS DEVELOPERS ALREADY USE

For application consumption, it offers all [restful APIs](#) that developers already use to enable modern cloud apps, as well as mobile apps, and supports traditional crypto interfaces such as KMIP, PKCS#11, JCE, CAPI and more enabling easy application integration. For C/C++ programmers, solution provides a PKCS#11 interface through [library](#). Java programmers can access the platform through the [JCE interface](#) and through Java SDK



HIGHEST LEVEL DATA SECURITY WITH HSM ACCESS

With a FIPS 140-2 level 3 certified appliance, encryption keys and tokens get the highest level of security. Tamper resistant hardware enables developers to execute sensitive code inside the secure execution environment of an HSM.

Solution Highlights

- **CENTRALIZED KEY AND POLICY MANAGEMENT.** Fortanix enables centralized key management and control of application-layer encryption.
- **ADD TOKENIZATION LAYER.** The combination of Format Preserving Tokenization and role-based access control (RBAC) for applications helps in protecting sensitive data.
- **SUPPORTS REST APIS AND COMMON PROTOCOLS.** Developers can utilize REST APIs and common encryption protocols like PKCS#11, CNG, JCE etc. to effectively implement encryption to app.
- **ROLE BASED ACCESS CONTROLS.** Integrates with SSO and supports RBAC. All sensitive operations such as enrolling applications, key generation or usage require authentication.
- **FLEXIBLE DEPLOYMENT OPTIONS.** Solution is available as a software, SaaS, and hardware appliance.
- **CONSOLIDATED AUDIT LOGGING.** Secure, comprehensive audit logs to help meet compliance.

How it works

By utilizing REST APIs and common encryption protocols like PKCS#11, CNG, JCE etc. developers can effectively implement encryption to app. Identity access management with single-sign on, active directory integration, role-based access control, with secure, comprehensive, tamper proof audit logs, provide insight into how data is being used, helping meet compliance requirements.

