Fortanix®

Solution Brief

AWS External Key Store (XKS) with Fortanix DSM

Move workloads with privacy-regulated data to the AWS platform with Fortanix Data Security Manager (DSM). DSM is a centralized key manager to create, store, and track your encryption keys separately from the data in the cloud. Fortanix DSM as an external key manager helps organizations with security and privacy regulations such as the GDPR and Schrems II.

Overview

Regulations like the Schrems II ruling and the GDPR require organizations to ensure PII data from citizens in the European Economic Area (EEA) remains within these borders. This data must be protected using state-of-the-art encryption, and the encryption keys must be in the sole custody of the data importer. In addition, these regulations require the ability to revoke data access at any time, and to segregate encryption keys from data on the cloud. An external key store—sometimes called a Bring-Your-Own-Key-Management-System (BYOKMS)—introduces an extra encryption layer to give organizations full custody of their keys. With Fortanix DSM, organizations can centrally manage the key lifecycle, and enforce granular access control and comprehensive logs to simplify the auditing process.

The decryption key is in the sole custody of the protected data importer, and, possibly, the exporter itself or another entity trusted by the exporter that is located in the EEA or a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA, and appropriately secured against unauthorised use or disclosure by technical and organisational measures conforming to the state of the art

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Fortanix Solution

Fortanix DSM functions as an AWS external key store to enable organizations to move the data to the cloud with the highest level of security and control for their keys. Encryption keys are under complete customer control and secured by FIPS 140-2 level 3 certified HSMs, segregated from the cloud data. Fortanix DSM users get a centralized solution to get control of the lifecycle of their keys, no matter if they are used on-premises, or in the cloud. Because Fortanix DSM users have sole key custody, neither Fortanix nor AWS can enable access to the protected data, not even when a government subpoena is issued, for example through the CLOUD act.

Key Features and Benefits

GDPR/Schrems II Compliance

By using Fortanix DSM as a centralized, external key store, users maintain full custody of their keys and gain full control over the data encryption policies within AWS. This control includes defining where the keys reside, and from where they may be accessed. DSM provides granular audit logs, so the customer can easily prove to auditors that regulated data remains within the EEA, and that they comply with regulations such as the GDPR, including restrictions defined by the Schrems II ruling.

Multicloud KMS Simplicity

Fortanix DSM provides a single and secure source to protect keys and data, regardless of whether they are used on-premises, or in the cloud. Define, enforce, and track data access policies from a single interface, and accelerate cloud migration. DSM provides granular, role-based policies, including quorum approvals, and integrates seamlessly with existing authentication identity providers.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Complete Customer Control

Organizations that want to fully control their risk must have full control of the keys that protect their data. By using the KMS solution from their cloud provider, they trade proximity for exclusive control. A court order can force cloud providers to hand over keys and data. With DSM as an external key store, organizations have full control and ownership of their keys and data. Fortanix DSM also provides a kill-switch functionality. This allows administrators to immediately block access to data-at-rest on the AWS platform with just a couple of clicks to change permissions for any, or specific, instances and locations.

Automated Key Management

Automate the complete key lifecycle from generation, rotation, expiration, to revocation to ensure secure and consistent key management across on-premises and (multi)cloud environments. DSM provides state-of-the-art automation features like automatic key rotation, one-click rotation across regions and clouds, automatic key expiration-based key rotations, and automatic alerting based on key state changes.

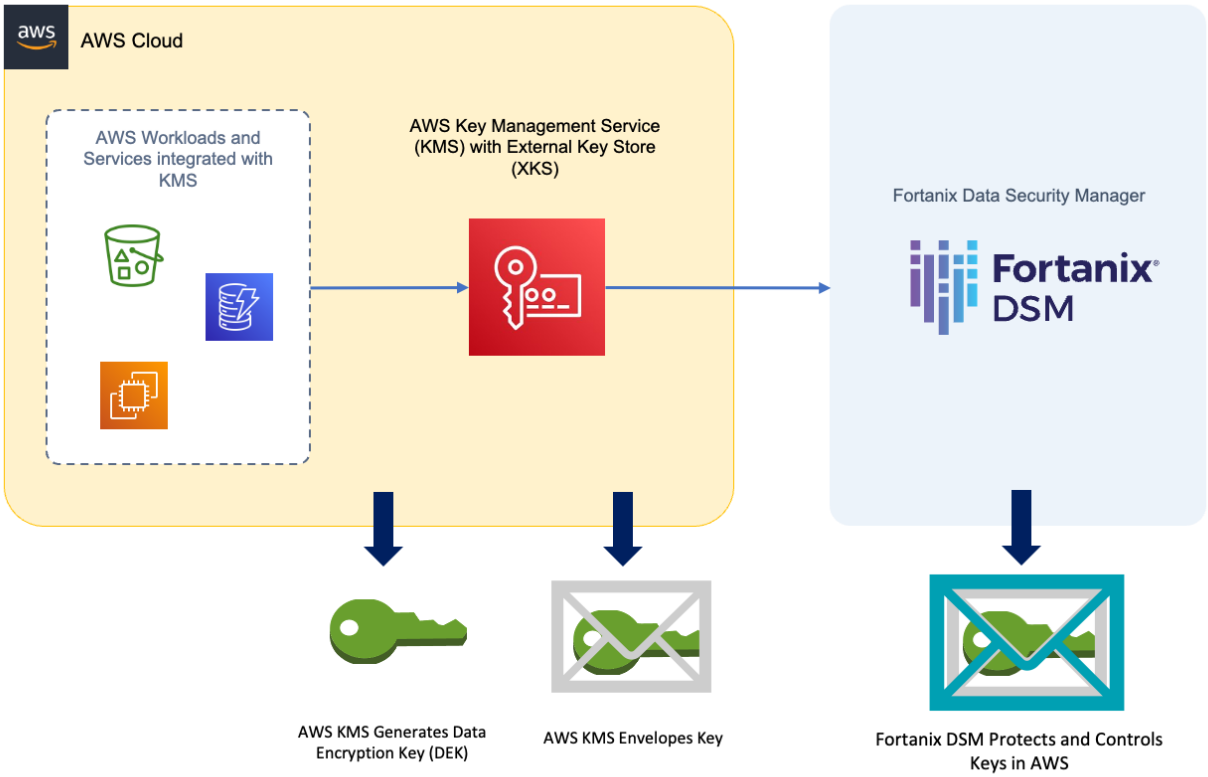
Secure and Flexible Deployment

Fortanix DSM is available as a SaaS platform, and as a physical or virtual appliance to best fit your environment. No matter your deployment preference, keys are protected by FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs) and neither AWS nor Fortanix have access to them. Data-in-use is continuously protected by Intel® SGX Secure Enclave technology.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

How Does AWS External Key Store with Fortanix DSM Work?

As shown in the diagram below, XKS allows AWS KMS to use external, customer-managed Root Keys, which increases the customer's control of their key management and data protection initiatives.
The customer's Root Keys are generated, protected, and used wholly within Fortanix DSM. AWS KMS calls DSM to unwrap Data Encryption Keys (DEKs) for use by the AWS services it supports. DSM enforces granular access control and key usage policies. DEKs protected by an XKS are doubly enveloped (encrypted): once by KMS, and once by DSM. Every time the key is used by a KMS client, KMS requests Fortanix DSM to open the blue envelope and we send the gray envelope back to them to decrypt. This way, Fortanix never sees the customer's keys.



Summary

With Fortanix DSM, users can simplify their key management across hybrid multicloud environments by taking ownership of their keys, and their data. By moving the root of trust away outside the cloud platform, organizations can ensure restricted data remains within a designated region and prove this to auditors. In addition, centralizing key management streamlines management processes and allows organizations to freely migrate workloads between regions or even between clouds. Fortanix DSM easily integrates with cloud providers such as AWS KMS as well as Google Cloud Platform.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040