Fortanix®

Case Study

Global IT Leader Achieves Security and Compliance with Fortanix Cloud-first, DevOps friendly solution

Customer Profile

Fortune 100 company and a leader in IT and networking. The company develops, manufactures, and sells networking hardware, software, telecommunications equipment and other high-technology services and products.

The Multi-Cloud Data Security and Compliance Challenge:

With data spread across multiple cloud environments including Amazon S3, RDS and Azure, the security of organization's data and keys was heavily reliant on the cloud native HSMs. With each cloud native HSM adopting a different approach and mechanism to manage encryption and keys, it was becoming increasingly complex for the security teams to manage and control the data lying across these dispersed cloud environments. To add to the complexity, they were also using SQL and PostgreSQL databases.

Lack of visibility and control over encryption keys

With multiple systems to manage, security teams often lacked an overarching and centralized visibility into data usage and control over encryption keys. This prevented security teams from accurate and timely reporting to meet compliance obligations.

Cloud migration and compliance

The Company was also embarking on a project to migrate the sensitive workloads to Google Cloud (GCP), utilize the Big Query based data lake and meet necessary compliance requirements. Google Cloud provided the External Key Manager capability which allowed organizations to control cloud encryption keys outside the cloud environment. Controlling keys outside of the cloud environment was critical to meet compliance.

DevOps security

The pre-existing cloud native HSM/KMS systems did not support Rest APIs, modern DevOps tools and was not CI/CD ready. This meant it was not possible to integrate security into DevOps and made it much more complex to manage security

What Were They Looking For? - Key Requirements

Increased adoption of multicloud had fragmented data across different public clouds. And that made securing data more complex. To guarantee universal protection of cloud data, security and cloud teams needed to get control and visibility of all data from a single pane of glass. Specific requirements were as follows-

Cloud first single management FIPS 140-2 Level-3 HSM to provide Key Management Services for compliance.	An external KMS that integrated with GCP's External Key Manager capability	Provide the Cloud infrastructure team with a tool that is easy to use and offers Terraform-based automation.
A highly scalable service that offers ability to scale/auto-scale to hundreds of millions of keys.	Business Continuity Process (BCP)/Disaster recovery (DR) that offered a high percentage of SLAs.	And most importantly it needed to be a DevOps friendly tool that offered easy and seamless integration with Splunk for logging and other DevOps tools.

What was offered? - Fortanix Solution

Fortanix Data Security Manager (DSM) SaaS provided integrated data security with encryption, multicloud key management, tokenization, and other capabilities from one platform, delivered-as-a-service. The phase one of the project included migrating to GCP and utilized Google Cloud External Key Manager (EKM) interface to manage encryption keys in Fortanix. Further the company expanded the use case to AWS cloud. Fortanix solution was used to manage keys generated in cloud, as well as for Bring/Hold-Your-own-Key (BYOK)/HYOK across all clouds

Fortanix solution was available across AWS, Google Cloud and Microsoft Azure, supported consistent encryption key management policies across multiple cloud providers, tenants, and regions while also enabling keys from any cloud or on-premises HSM to encrypt data anywhere. The platform catered to the need of secure and automated key management with zero downtime for modern development and deployment lifecycle with additional features like Tokenization and Secrets Management to address problems faced by DevOps as well as Security admins in a multi-cloud environment. The high-level design included the following Fortanix components:

- Data Security Manager (DSM) FIPS 140-2 Level-3 Hardware Security Module and management layer for CSP HSMs via HSM Gateway.
- Support for Transparent Data Encryption for Database Encryption at rest, including for SQL Server and Postgres
- Support for #PKCS11, MS CAPI, MS CNG, Java JCE, KMIP interfaces and other libraries
- Single UI / Endpoint for easier access
- Automated Load-Balancing / High-Availability

Why Fortanix? - The key differentiators?

DEVOPS-FRIENDLY

- Fortanix provided a DevSecOps platform that automates secrets via Terraform/GitHub
- Allowed them to create and enforce policies around Key/Secrets Management
- Rolling updates provided an interruption free update process
- Native Splunk integration for logging
- Provided most common interfaces to serve DevOps tools

EASY TO DEPLOY AND SCALABLE

- Fortanix offered a SaaS based model that was quick to deploy
- Linearly scalable solution had the capability to store hundreds of millions of keys in one single cluster.
- Offered additional features like Key caching to accommodate high volume of transactions and outperformed traditions KMS/HSM.

HA/DR READY PLATFORM

- Backup and Disaster Recovery for keys stored in AWS CloudHSM and Azure Key Vault Managed HSM.
- High availability with a minimum of 99.9 SLA.

The Impact

Fortanix solution has helped redefine the data security posture of the IT Leader. With increasing cyberattacks, the battle to defend company information and assets in the cloud and on-premises was never ending. Fortanix solution offered scalable, simple to use and a unified experience across different cloud/hybrid environments, providing virtually impenetrable security to data, keys, and secrets. Core benefits included-

Cloud Key Management with single pane of glass provided centralized visibility and control.

Security Team got full visibility, control, and provided ease of reporting, and compliance as the they migrated more data and workloads to Cloud.

With the DevOps-friendly solution, it was now possible to integrate data security into the CI/CD pipeline and create a truly secure development environment.

Fortanix®

About Fortanix

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks. For more information, see **www.fortanix.com**

REQUEST A DEMO