



## Fortanix helps a global Fintech leader achieve seamless and secure cloud migration.

Fortanix allows the Fintech Company to pick the right level of data controls depending on business use-case and required security posture

### Customer Profile

World leader in online payment systems enables any business or individuals to securely transact, send and receive payments online.

### Fintech Cloud Data Security and Compliance Challenge

Like many financial services firms the company's infrastructure had traditionally been on-premises. However, as business grew, they wanted to migrate from datacenters to the cloud. Following a detailed RFP, and an in-depth technical review of all the leading platforms they chose Google's Cloud Platform (GCP). For data security, they relied on existing 'rack and stack' HSM infrastructure that was built to protect on-premises data in the confines of a traditional data center. With a strategic need to migrate workloads and data to the cloud, it was important for them to revisit their data security. They needed a way to protect the data from getting compromised.

This prompted them to look for a solution that could give them the same level of security and control over data and applications in the public cloud as they would running on-premises. Existing HSM solutions have typically treated on-premises data security and cloud data protection as two separate problems with two separate solutions delivered on two separate technology stacks. Moving from one to the other is very difficult, making cloud deployments almost impossible. Traditional solutions are also not able to provide control and as-a-service option with strong SLAs.

Cloud native encryption relies on the Cloud Service Provider (CSP) to secure data and is offered as the default data encryption method to the customer. Cloud providers generate and own the data encryption keys directly. GCP encrypts customer data-at-rest by default using its native key management and encryption. From a security standpoint, this was the easiest method to implement, but it did not provide adequate controls over encryption keys. They also had to meet specific compliance regulations for data security. Many of these regulations require the organization to store the cloud keys outside the Cloud Service Provider's (CSP) platform to prevent insiders and cybercriminals from gaining access to the keys and in turn to sensitive data.



**Existing HSM solutions were an impediment for cloud migration.**



**GCP's cloud native encryption did not offer adequate control -- or ownership of keys to the customers**



**Meeting compliance was a challenge**

Enhanced control and ownership over their encryption keys was required to meet compliance and internal security requirements for certain types of sensitive data/workloads.

## What Were They Looking For? - Key Requirements

### SAAS BASED DATA SECURITY TO ENABLE CLOUD MIGRATION

The main focus for them was to get a solution, preferably a SaaS solution, that allowed to securely migrate workloads/data to the cloud and enabled them to pick the right level of data control depending on data classification and with the ability to store keys outside of GCP to meet a critical compliance requirement.

### ABILITY TO INTEGRATE WITH GCP'S EXTERNAL KEY MANAGER CAPABILITY

Bring your own KMS is another approach (also known as GCP External Key Manager), which is only supported by GCP today. This approach allows organizations to store the keys outside the GCP infrastructure and within an external third-party KMS. The primary benefit from this approach was that the Key management service resided completely outside the control of GCP giving organizations greater control over the data and with no access of master keys to GCP. They also got the ability to revoke the access to master keys making the data completely inaccessible when required.

The Company chose Fortanix integrated data security as a service platform that also offered the ability to Bring-Your-Own-Key-Management-System (BYOKMS) for GCP. Fortanix Data Security Manager (DSM) SaaS offers integrated data security as a service that provides secure key management and cryptography services including cloud key management, secret management, and tokenization to protect sensitive data in public, private, hybrid, or multi-cloud environments. Encryption keys are stored in the FIPS 140-2 Level 3 certified HSM and cryptographic operations are securely executed within the module.

## What was offered? - Fortanix Solution

### Comprehensive protection with the Integrated Data Security as a Service Platform

The company had classified all its data into multiple categories based on the business use-case, sensitivity of data and defined rules on how this data should be processed, where it should live and the extent to which the data needs to be owned and controlled. They have deployed Fortanix HSM as a service globally in all regions. All their internal applications and data leverage Fortanix for data security either through the service directly or through Fortanix integration with Google Cloud Platform's (GCP) External Key Management service. Whether to bring their own encryption keys (BYOK) and let GCP do the crypto or allow them to bring own keys as well as own the crypto (BYOKMS/BYOE), Fortanix offered the flexibility to adopt the security posture based on the data type and controls required.

With a comprehensive Data Security as a Service (DSaaS) platform, from Fortanix, offering integrated hardware security module (HSM), key management, encryption, shared secrets, and tokenization capabilities, the company was able to meet a broad set of use cases from a single platform, lowering the TCO and offering comprehensive security for all types of data and workloads. The company was able to operate even the most sensitive applications in any environment. The Fortanix solution was also capable of effective scaling and clustering between global sites allowing deployment of the solution across all regions and sites. The high-level design included the following Fortanix components:

- ✓ **DSM FIPS 140-2 Level-3 certified HSM:** Data Security Manager (DSM) FIPS 140-2 Level-3 Hardware Security Module and management layer for on-prem HSMs via HSM Gateway.
- ✓ **Bring Your Own Key-Management-System (BYOKMS):** Ability to manage and control encryption keys outside GCP with Fortanix (Bring Your Own Key-Management-System (BYOKMS). Fortanix solution integrated with Google Cloud Platform's External Key Manager service to enable them to move the data to the cloud and get the same level of security for keys that they are used to, in their own on-prem environments. Keys for encryption are never stored at GCP. They are always under the control of the company, away from the cloud. With a click of a button, in real time, the organization can enable and disable access to data from specific instances and locations.
- ✓ **Kill-Switch capability:** Fortanix provided a kill switch, which allows them to stop decryption of data-at-rest in GCP services by simply disabling their key in Fortanix KMS. As the key never leaves Fortanix, they get complete control of how to authorize the use of the Google Cloud's External Key Manager keys. This level of control that Fortanix provides has never been available to customers adopting public cloud. This is an extremely powerful feature for many customers who would like to be in control of their data even when they make it available to public cloud. The customer gets complete control of how to authorize the use of the Google Cloud's External Key Manager keys.
- ✓ **Bring Your Own Encryption (BYOE):** When client-side encrypted data stored in the cloud needs to be consumed by cloud-native services, the Fortanix KMS transparently transforms data from client-side encryption (DEK owned by the company) to server-side encryption (KEK owned by GCP). Cloud-native services can then consume the data and perform required operations before the data is re-encrypted using the customer's keys. Fortanix offered the most secure and comprehensive solution in this category and was the first solution that allowed customers to own all keys and continue to use cloud-native services that required access to the data.
- ✓ **Unified Policy Management:** Consistent policy management across clouds, tenants, and regions.
- ✓ **Cloud Encryption Key Backup and Disaster Recovery:** Back up, restore, and re-import master encryption keys for public cloud KMS.
- ✓ **Cloud and DevOps Friendly API:** All security functions were supported as RESTful APIs, for easy integration to cloud-native tools and technologies.

## Why did they choose Fortanix? Key Differentiators



### Seamless Integration

Fortanix offered seamless integration with GCP's External Key Management Service.



### Available as a Service

The solution can be consumed as a service which was best suited for their infrastructure and cloud migration plans.



### Flexibility

Fortanix offered great flexibility in terms of the security controls that could have been offered depending on data types and use cases.



### Complete Control of Keys

Fortanix provided them with a kill switch, which allows them to stop decryption of data-at-rest in certain GCP services by simply disabling their key in Fortanix KMS.



### Simplified and Centralized Encryption

Fortanix provided a single, simple, and centralized encryption platform that accelerates moving applications to public cloud, while providing a single set of cryptographic services to on-premises, hybrid, and cloud workloads.

## The Impact

With different types and categories of data, it was critical to have a solution that would offer the flexibility to manage data based on its use cases and specific controls required. Fortanix allows the Fintech Company to pick the right level of data controls depending on business use-case and required security posture.



### Secure cloud migration

The solution enabled new business use cases to go to the cloud environment. The Company was able to choose from varying degrees and levels of data control depending on what type of data it is. And with some data not enabled for cloud type services, BYOKMS capability allowed them to potentially bring those into the cloud environment as well. This helped migrate additional use cases to cloud.



### Achieve compliance

Fortanix helped meet compliance by allowing them to manage their own keys and secure them by storing them in FIPS 140-2 Level 3 certified hardware security modules (HSMs).



## 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](https://www.fortanix.com)

REQUEST A DEMO