ZIMPERIUM®

Securing Cryptographic Key Management during Cloud Migration

Industry
Banking

Location
Global company based out of the United States

Solution
zKeyBox
zShield

Customer Profile

This Fortune 100 integrated payments company offers seamless and secure payment options across the globe. The company places an emphasis on digital innovation that enhances the customer experience and provides safe, reliable, and convenient methods of payment processing for customers and merchants.

The Challenge

The company needed to address the challenge of securely managing cryptographic keys during their migration from expensive on-premises data centers to their multi-cloud infrastructure. While making the transition to the cloud, they needed to ensure data security and faced a decision regarding the management and ownership of cryptographic keys moving forward. They did not have dedicated hardware provisioned for the company on the cloud. Instead, its keys would be stored in virtual machines, potentially making them vulnerable to shared underlying hardware. In addition, the encryption algorithms and key refresh cycles were primarily determined by the cloud provider, leaving them with reduced control over their data security posture. If they chose to manage their keys using a cloud provider's Key Management System (KMS), they would still be responsible for safeguarding the keys as the provider would not assume liability. Therefore, if the keys were lost and not retrievable, the company needed to store a copy in a secure on-premises vault. Entrusting key management to the cloud provider meant granting them access to the keys, which understandably raised security concerns.

The Solution

Seeking an autonomous and complete security solution, the company elected to develop its own on-premises KMS. They developed a key management SDK, which served as the interface for all applications to access the keys. This component became a common feature across enterprise applications, providing a standardized and secure method of accessing cryptographic keys. As a critical component of the SDK, Zimperium's cryptographic key protection solution, zKeyBox, was responsible for securing the keys while they were being retrieved and used by applications leveraging the SDK. Keys were protected at rest, in motion, and in memory with zKeyBox. This ensured that the keys remained owned by the organization and would remain protected throughout their lifecycle. To further enhance the overall security of the SDK, they implemented Zimperium's award-winning application shielding solution, zShield. This added a protective layer that safeguards the integrity of the SDK's code and prevents unauthorized access and tampering attempts.

Impact

By combining its own on-premises KMS with Zimperium's zKeyBox and zShield to secure its cryptographic key management, the company overcame the barrier that previously hindered its applications' migration to the cloud. They have been able to leverage the benefits of cloud infrastructure while maintaining robust data security measures. By retaining control over their cryptographic keys, they eliminated concerns about sharing underlying hardware and improved their data security posture. They also ensured they were in alignment with industry-specific compliance requirements and regulatory standards. Realizing the full potential of mobile-forward business puts the company in a position to achieve even greater results going forward!

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244