cpl.thalesgroup.com

THALES
Building a future we can all trust

Major North American Bank Improves Compliance and Simplifies Data Security across Hybrid IT

A major North American bank forecast substantial financial risk brought on by burgeoning cybercrime and resulting possible non-compliance with government regulations and industry mandates. Consequently, the bank proactively resolved to significantly strengthen its digital security posture to avoid the very real likelihood of lost customer business and even fines should a data breach occur, or should the bank fail a compliance audit.

Challenge

This North American bank was concerned the complexity of its hybrid infrastructure, including a network of private and public clouds, SaaS platforms, and legacy on-premises systems, could lead to a lack of visibility into the disposition of sensitive data across its systems and lack of control over security policies. This could become a major challenge given the multiple privacy, data security, and data sovereignty regulations the bank is subject to.

To ensure optimal data protection and compliance with regulations, the bank's digital security team wanted to implement a centralized approach to data security governance. The team saw its challenges as:

- Complying with financial services regulations, such as PCI DSS, FIPS, NYDFS, and privacy legislation, such as GDPR and CCPA.
- Simplifying the complexity of key management for multiple third-party security platforms and gaining control over the bank's bring your own key (BYOK) keys.
- Reducing the complexity of security and data protection in multiple on-premises and cloud environments.

Solution

Complying with virtually every financial services data security regulation in the industry requires pseudonymization of data and tight control of the cryptographic keys that return the pseudonymized data to its original form. This is very complex when the pseudonymized data is spread across legacy, on premises, and multiple cloud storage environments, and employees and customers in multiple locations need access to the data.

The bank decided to work with Thales, because it has decades of experience with every aspect of data security the bank wanted to address.

Complying with virtually every financial services data security regulation in the industry requires pseudonymization of data and tight control of the cryptographic keys that return the pseudonymized data to its original form. This is very complex when the pseudonymized data is spread across legacy, on premises, and multiple cloud storage environments, and employees and customers in multiple locations need access to the data.

Encryption

The bank deployed Thales's CipherTrust Data Security Platform using CipherTrust Transparent Encryption to pseudonymize data in all formats across multiple data stores. CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control, and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. Agents are installed at operating filesystem or device layers, and encryption and decryption are transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost.

Cryptographic key management

The CipherTrust Data Security Platform also enabled the bank to centralize cryptographic key management for all platforms including Azure, AWS, Salesforce, NetApp storage encryption, CyberArk, and third-party data centers. Using CipherTrust Manager with a Luna hardware security module (HSM) as root of trust, the bank enacted on-premises key management for all third-party solutions, including TDE and KMIP. This converted their BYOK control problem into a secure hold-your-own-key (HYOK) solution.

CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly REST API.

Root of Trust

Luna HSMs are hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures. Luna HSMs are certified at various FIPS 140-2 Levels and are used to:

- Meet and exceed established and emerging regulatory standards for cybersecurity
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

Luna HSMs are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations.

Results

According to the executives in the bank, they viewed the CipherTrust Data Security Platform as a "Multi-purpose encryption survival tool" that enabled the bank to:

- Elevate its compliance profile through centralized data security enforcement across Hybrid IT from CipherTrust's single pane of glass monitoring and control console.
- Simplify and increase the security of keys and key management of multiple third-party security platforms and cloud environments.
- Centralize cryptographic key management on-premises and extend it to cloud environments. This meant the bank had complete control of its keys reducing the likelihood of a breach in the cloud.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us