cpl.thalesgroup.com

THALES
Building a future we can all trust

Global Mobile Network Operator Deploys Portfolio of Thales Solutions as Centralized Data Security Solution for Entire Enterprise

Introduction

A global mobile network operator (MNO) wanted to revamp their cyber security posture and implement best-in-class security for sensitive customer and business data across the enterprise, improving compliance and reducing the risk of a data breach.

Challenge

After assessing the needs of cloud and on-premises systems used by multiple business units, the MNO decided to implement a centrally-managed enterprise data security solution that could be tapped by several internal customers.

The chosen solution would have to support several use cases to protect sensitive data as it flows through multiple systems and is used by applications and users in different business units. These included:

- Secure root of trust for code signing, certificate management, and PKI
- Key management for multiple cloud, hybrid, and on-premises environments
- Encryption of sensitive data stored in databases and file systems
- Pseudonymization of sensitive structured data in databases
- Payment transaction security for a network of retail stores and e-commerce

Solution

Serving as trusted advisor, Thales helped the customer understand its business and technical needs and how to implement data security best practices. After considerable research and proof of concept (PoC) tests measuring the breadth of capabilities, performance, ease of implementation, centralization of security policies, and scalability, the customer chose Thales to provide a comprehensive data security solution.

The company implemented a centralized data security solution from Thales, available for the entire enterprise. Business units can tap into the multiple capabilities available in a data security stack to address their specific use cases ranging from key management to pseudonymization and payment transaction security, resting assured that their cryptographic keys are securely stored and managed throughout their lifecycle.

Luna Hardware Security Modules

Thales Luna Hardware Security Modules (HSMs) were deployed on-premises to protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, FIPS 140-2 Level 3 tamper-resistant device. Luna HSMs can be deployed on-premises, in the cloud, as a service, or across multiple environments to support hybrid infrastructure and can help simplify integration with a wide variety of APIs and the broadest partner ecosystem in the market. Companies can quickly secure hundreds of applications with Luna HSMs out-of-the-box technology partner integrations. The company was able to leverage the Luna HSM integration with CyberArk to securely manage business application credentials like passwords and the integration with Garantir to securely store the keys used for code signing. Luna HSMs safeguard the private keys and associated certificates used by enterprise business applications as well as the keys that are used to authenticate the endpoints involved in TLS operations. Luna

Thales solutions were deployed as a centralized data security solution for the entire enterprise. Any business unit can leverage the data security stack to address use cases including secure key management on premises or in the cloud, data-at-rest encryption, pseudonymization, code-signing and payment transaction security.

HSMs are ideal for use cases that require high performance such as the protection of SSL/TLS keys and high volume code signing.

Luna HSMs were also selected to provide a secure root of trust for Thales CipherTrust Manager, the encryption key management solution the company also deployed, ensuring crypto keys are protected throughout the entire lifecycle.

Crypto Command Center

Thales Crypto Command Center – a crypto hypervisor – was deployed to provide one complete, centralized solution for the management of crypto Luna HSM resources. With it the customer can deliver on-demand provisioning of crypto resources for data protection in minutes instead of days, while allowing application and data owners to maintain full control of crypto services and data.

CipherTrust Data Security Platform

The CipherTrust Data Security Platform was selected to simplify data security administration and accelerate time to compliance. The customer's use case implemented three of the platform's integrated solutions to provide comprehensive protection and centralized key management for sensitive data in the cloud and on-premises.

CipherTrust Transparent Encryption with Centralized Key Management

CipherTrust Transparent Encryption was implemented to protect file systems and databases in multiple environments. CipherTrust Transparent Encryption includes centralized policy and key management, granular access controls that allow only authorized users and processes to decrypt specified data when needed while keeping all sensitive data encrypted, and detailed data access logs required for audits. The agent is installed at the operating file system or device layer to protect data in files, volumes, databases and servers in the cloud or on-premises, making deployment simple, scalable and fast.

CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager was selected to centralize and automate key lifecycle management across the enterprise's Amazon AWS, Google Cloud, and Microsoft Azure environments. The solution provided the MNO with a single user interface for simplified management and control over their cloud native, bring-your-own-key (BYOK) and hold your-own-key (HYOK) keys managed on-premises with HSMs guaranteeing high entropy key generation and secure key storage.

CipherTrust Cloud Key Manager enables key generation, usage logging, and reporting, and facilitates 'key decoupling' by securely storing the keys separately from the encrypted data. These features provide customers with control over the encryption keys used to encrypt their data in the cloud and are considered industry best practices.

Centralized data security solution

- All business units can tap into the multiple capabilities available in a data security stack to address their specific use cases ranging from secure cryptographic key management to pseudonymization and payment transaction security.

Reduced risk of data breach

- Reduced the risk of a data breach by enabling all business units to protect all the most important systems that store or process sensitive data across the enterprise.

Quick time-to-compliance

- The fast implementation of a comprehensive data security infrastructure enabled a quick time-to-compliance with industry mandates such as PCI, and regulations such as FIPS.

Benefits of scale and lower cost

- The enterprise was able to reduce cost by making the entire security infrastructure available to all business units and replacing ineffective point solutions.

Tokenization with Dynamic Data Masking

To protect structured data in databases, Thales implemented CipherTrust Tokenization with dynamic data masking. This solution permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without the exposure of sensitive data during the analysis or in reports.

payShield Payment Hardware Security Modules

payShield HSMs were deployed to protect in-store payment transactions at thousands of retail points of sale (POS) and at the main company e-commerce web site. payShield from Thales is the world's leading payment HSM, helping secure an estimated 80% of global POS transactions. As the HSM of choice for payment solution providers and payment technology vendors, it delivers proven integration with all leading payment applications. payShield addresses the latest mandated security requirements for a wide range of organizations including EMVCo, PCI SSC, GlobalPlatform, Multos, and ANSI.

Results

Thales's commitment to advise the customer security best practices practices, deploy internal resources to understand customer needs, and prove Thales capabilities in PoCs was key to build trust and allow for a seamless deployment of multiple solutions.

By leveraging Thales data security products as a centralized data security infrastructure the MNO achieved an immediate reduction in the risk of a data breach with comprehensive best-in-class capabilities covering multiple use cases. The enterprise was also able to reduce cost by making the entire security infrastructure available to different business units and replacing ineffective point solutions.

The fast implementation of a comprehensive data security infrastructure also enabled a quick time-to-compliance with industry mandates such as PCI, and regulations such as FIPS, protecting the privacy of millions of subscribers and confidentiality of corporate customer data.

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