Thales Helps University To Secure Sensitive Medical Research Data

Overview

This leading Australian research university was founded in 1958 and is home to major research facilities for science, law and medicine. Consistently ranked amongst the top 75 universities in the world, this university has campuses spanning 3 continents.

Business Challenge

Being a research facility, this university collaborates with a number of medical facilities, collecting a lot of sensitive medical data for assessment and research purposes. The various sources of sensitive medical data are stored in data warehouses in different locations. With all these sensitive data, this university recognised the need to protect these sensitive data while needing to comply with local privacy regulations.

Technical Challenge

This university deployed several open source encryption solutions to protect their sensitive medical data at rest and in-transit. However these open source encryption solutions posed a number of challenges, including:

- The lack of product development roadmap and so these open source solutions are not future proofed
- The university needed to deal with various solution providers which caused high overheads for internal resources to maintain and support
- The open source solutions deployed do not have any security accreditation
- The open source encryption solutions do not offer the ability to separate the encryption keys from the encrypted data

The solution

To meet the university's challenges, Thales proposed a Data Security Manager (DSM) solution to securely manage the university's encryption keys in various environments.

With DSM, the university is able to manage the full lifecycle of all their encryption keys, including secure key generation, backup/restore, clustering, deactivation and deletion. More importantly, this allows the university to have additional security by being able to separate their encryption keys from their sensitive data stored in various VM clusters and database servers.

Result and Benefits

The solution that the university adopted not only met its immediate requirement to manage their encryption keys but also has the flexibility and scalability to cater for the university's future requirements such as:

- Centrally manage additional encryption keys as they expand data storage into other physical and or cloud environments
- Implement Bring Your Own Keys (BYOK) or Bring Your Own Encryption (BYOE) when moving to the cloud
- Using DSM's transparent and application encryption capabilities to protect their sensitive data
- Being able to meet compliance requirements such as FIPS 140-2 levels 1-3 certification

Business Need:

- The ability to separate their encryption keys from their data stored in different environments
- To be able to deal with a single solution provider for management of all their encryption keys

Technology Need:

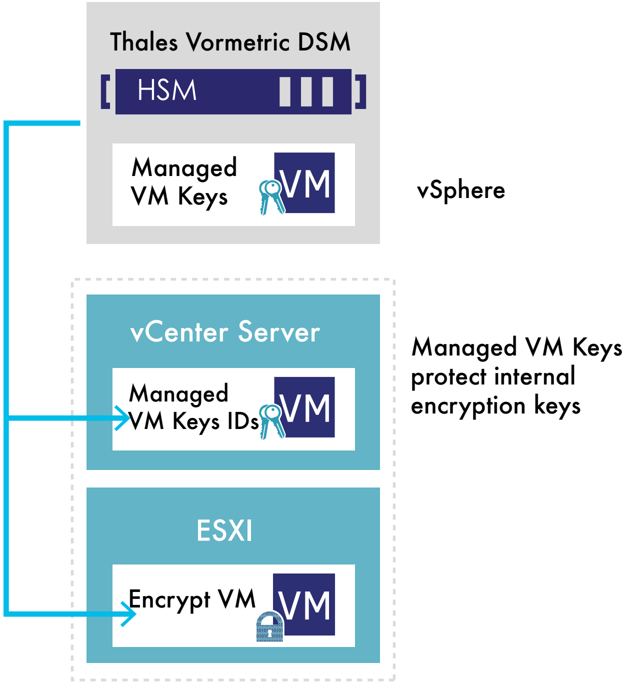
- Solution to manage the full lifecycle of all their encryption keys
- To have a solution with a clearly defined development roadmap to meet the university's future requirements

Solution:

- Thales Data Security Manager (DSM)

Result:

- World-class encryption key management implementation capable of supporting the university's changing requirements
- A solution that enables centralised management of data security policies and key management, simplifying training, deployment and operations



About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations 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.

> cpl.thalesgroup.com <

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