Global Bank Case Study

Encryption and Centralized Key Management Project

Client Overview

- The CISO organization of the Bank, in response to an audit finding and in an effort to address forthcoming privacy and regulatory requirements, established an initiative to encrypt over 2,500 Oracle databases with Transparent Data Encryption (TDE).
- After evaluating multiple vendor products the decision was made to use Oracle Key Vault to handle critical key management tasks
- The first phase of the project focused on the design for a global implementation of Oracle Key Vault. Key deliverables:
  - Documentation and Validation of Client Requirements and Use Cases
  - High level global OKV architecture

How Our Consultants Helped

- Analysis to determine requirements, use cases and technology needs for a global centralized key management system
- Complete a design for Oracle Key Vault to manage keys for encrypted databases residing worldwide
  - High Availability
  - HSM integration
  - Manage keys for 2500+ databases
  - High level architecture
- Position the Bank for a Phase 2 project to include a low-level design and production implementation plan
  - Encrypt 2500+ Oracle databases
  - OKV installation with high availability and HSM integration
  - Roll-out schedule

Results

- CISO's Defense in Depth Strategy – Phase 1
  - Centralized Key Management solution required for encryption
- Addressed New York State's Department of Financial Services (NYSDFS) regulation
  - *23 NYCRR 500* - March 1, 2017 Encryption of Non-Public Information for data at rest
- Positioned the Bank to address GDPR (General Data Protection Regulation)
  - Takes effect May 25, 2018
  - Affects all entities doing business with EU citizens
  - Fines of up to £20 Million or 4% of global revenue

CROSSGEN