

# 아시아 태평양 지역 최고의 보험회사, 탈레스를 통해 디지털 트랜스포메이션 및 규정 준수 요건을 충족

## 탈레스 솔루션이 주요 비즈니스 과제를 해결하도록 지원

### 요약

아시아 태평양 지역 최고의 보험회사가 확장성이 뛰어난 탈레스 솔루션을 배포해 저장 중인 데이터를 보호하고 서로 다른 환경에 분산되어 있는 데이터와 키를 보호하고 관리하는 동시에, 어디에서 비즈니스를 수행하던 현지의 규정을 준수할 수 있는 모델을 제공하고 있습니다.

### 조직 소개

아시아 태평양 지역 최고의 금융 보안 그룹 중 하나로 알려진 이 회사는 구조적 성장 시장에 초점을 둔 아시아 최고의 비즈니스 포트폴리오를 구축했습니다. 생명 및 건강 보험 솔루션을 통해 고객을 지원하고 있는 이 회사는 싱가포르, 홍콩, 인도네시아, 한국, 일본, 베트남 같은 여러 국가에서 수 백만 명에 달하는 고객을 거느리고 아시아 태평양 지역에서 강력한 입지를 유지하고 있습니다.

이 회사는 현재 전 세계 40개 이상의 지점에 탈레스 솔루션을 배포하여 활용하고 있습니다.

### 비즈니스 요구

이 보험회사는 데이터 분석, 비즈니스 애플리케이션 및 인프라에서 클라우드를 활용하기 위해 디지털 트랜스포메이션을 추진하고 있습니다. 그러기 위해서는 확장성이 뛰어나고, 하이브리드 및 멀티 클라우드 환경에서 작동하며, 서로 다른 환경에서 데이터를 보호하고 키를 관리할 수 있는 솔루션이 필요합니다.

또한 이 보험회사에는 고객들에게 안전한 경로를 제공하여 규정 준수 요건을 충족할 수 있도록 지원하는 동시에, 데이터를 클라우드로 이동시켜 책임 공유 모델을 실현해야 할 의무가 있습니다.

반드시 준수해야 하는 규정은 다음과 같습니다.

- PDPA(Personal Data Protection Act)
- HIPAA(Health Insurance Portability and Accountability Act)
- PCI DSS(Payment Card Industry Data Security Standard)
- GDPR EU(General Data Protection Regulation)

### 과제

금융 부문에 종사하는 이 보험회사는 개인 데이터, 건강 관련 데이터 및 금융 데이터를 대량으로 취급하고 있습니다. 보험사로서 중요한 감사 요구를 충족하기 위해 규정 준수를 달성하는 동시에, 모든 고객 데이터를 유출되지 않도록 보호해야 하는 법적 책임을 지고 있습니다. 따라서 비즈니스가 수행되는 국가 현지의 개인정보보호법을 준수하지 않을 경우, 심각한 결과가 초래될 것입니다. 예를 들어 PCI 보안 표준 위원회(PCI Security Standards Council)에 따르면 규정을 준수하지 않는 그룹들은 막대한 법적 비용과 합의금을 부담하고 매출이 감소하는 불이익을 받게 됩니다.

탈레스는 여러 국가에서 비즈니스를 수행하고 있기 때문에 각국의 서로 다른 개인정보보호법에 대해 전략적 측면에서 고객에게 조언을 할 수 있습니다.

저장 중인 데이터 보호를 위한 도구를 제공하고 해당 데이터에 대한 키가 하드웨어 RoT(Root of Trust)에서 안전하게 생성, 저장 및 관리되도록 보장함으로써 기존 인프라를 개선하고자 이 보험회사가 선택한 최초이자 유일한 공급업체가 바로 탈레스였습니다.



## 솔루션

탈레스는 이 보험회사의 비즈니스 과정이 디지털 트랜스포메이션 및 규정 준수에 관련되어 있음을 파악했습니다. 이에 따라 다음과 같은 솔루션을 통해 저장 중인 데이터 보호에 필요한 도구를 제공하여 그룹의 보안 인프라를 개선하는 방법을 제안했습니다.

### 규정 준수 요건 충족 - 단계적 조치

개인 정보가 본질적으로 취약하다는 사실과 데이터가 사용, 저장 및 처리되는 방식을 고려할 때 데이터 보안은 필수적입니다. 데이터 보안 문제 및 개인정보보호 규정 요구를 충족하기 위해 HIPAA, GDPR 및 PCI-DSS 같은 데이터 보호 규정들이 제정되었습니다.

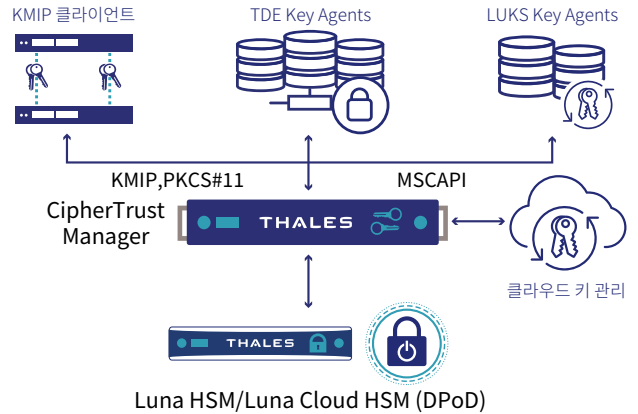
이 보험회사는 목표를 달성하기 위해 단계적으로 접근했습니다. 가장 시급한 1단계 조치는 규정 준수 요건을 충족하는 것이었습니다. 따라서 이 보험회사는 FIPS 140-2 레벨 3 인증을 획득하여 규정 준수 달성이 입증된 암호화 솔루션을 통해 데이터 보안 규정 준수 요건을 충족할 수 있도록 주문형 Thales Data Protection Luna Cloud HSM 서비스와 CipherTrust Manager를 선택했습니다.

- 주문형 [Thales Data Protection](#)은 온라인 마켓플레이스를 통해 다양한 Luna Cloud HSM 및 CipherTrust Key Management 서비스를 제공하는 클라우드 기반 플랫폼입니다 DPoD(주문형 Data Protection)을 사용하면 하드웨어를 구매, 배포 및 유지 관리할 필요가 없기 때문에 보다 간단하고 비용 효율적으로 데이터 보안을 관리할 수 있습니다. 필요한 보호 기능을 배포하고, 서비스를 프로비저닝하며, 보안 정책을 추가하고, 몇 분 내에 사용 보고서를 받아볼 수 있습니다. DPoD는 광범위한 클라우드 기반 Luna HSM 서비스를 제공하여 고객이 클라우드에서 데이터 암호화에 사용하는 암호화 키를 저장 및 관리하는 동시에, 다양한 사용 사례와 환경 전반의 통합 사례에서 키를 완벽하게 제어할 수 있도록 지원합니다. Luna HSM은 온프레미스, 클라우드 및 하이브리드 환경에서 하드웨어로 사용이 가능하고 FIPS 140-2 인증을 획득하는 등 보안이 강화된 변조 방지 어플라이언스 내에서 암호화 키와 기능을 안전하게 관리, 처리 및 저장합니다.
- [CipherTrust Manager](#)는 조직이 암호화 키를 중앙에서 관리하도록 지원하고, 세분화된 액세스 제어를 제공하며, 보안 정책을 구성할 수 있도록 지원하는 업계 최고의 엔터프라이즈 키 관리 솔루션입니다. CipherTrust Manager는 CipherTrust Data Security Platform의 중앙 관리 지점으로, 암호 키의 생성, 교체, 폐기, 가져오기 및 내보내기를 포함한 주요 수명 주기 작업을 관리하고, 키 및 정책에 대한 역할 기반 액세스 제어를 제공하며,

강력한 감사 및 보고 기능을 지원하고, 개발자에게 친숙한 REST API를 제공합니다.

물리적 어플라이언스와 가상 어플라이언스 모두에서 사용할 수 있는 CipherTrust Manager는 FIPS 140-2 레벨 3 인증을 획득한 Thales Luna HSM(온프레미스에서, DPoD를 통해 클라우드에서 서비스 형태로, 또는 하이브리드 환경 전반에서 함께 작동) 또는 타사 HSM(Hardware Security Module)에 통합되어 최고 수준의 RoT로 키를 안전하게 저장합니다.

### CipherTrust Enterprise Key Management



### 볼트가 필요하지 않은 토큰화(vaultless tokenization)를 통해 온프레미스에서 클라우드 인프라로 데이터를 안전하게 마이그레이션

2단계로 탈레스는 온프레미스에서 클라우드 인프라로 데이터를 안전하게 마이그레이션하기 위해 볼트가 필요하지 않은 토큰화의 사용을 제안했습니다.

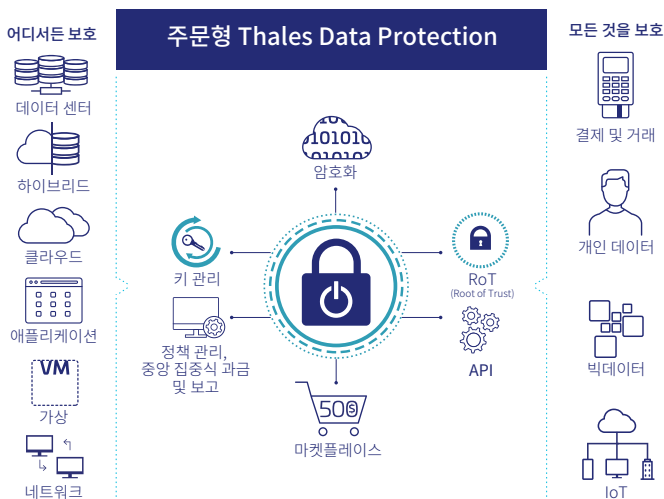
토큰화를 수행하면 EU의 GDPR(Global Data Protection Regulation), PCI-DSS(Payment Card Industry Data Security Standard) 같은 보안 정책 및 규제 명령을 준수하는데 소요되는 비용과 노력을 줄일 수 있습니다.

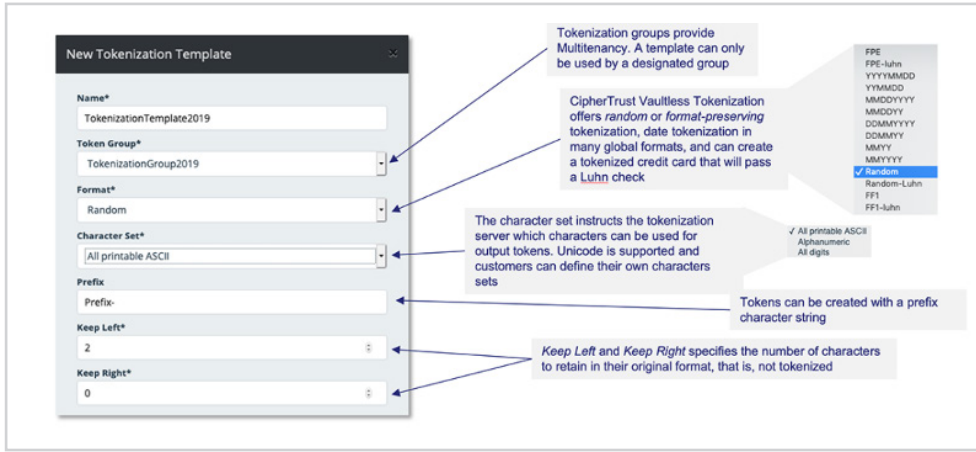
- [CipherTrust Tokenization](#)은 두 가지 형태의 편리한 솔루션을 통해 애플리케이션 수준의 토큰화 서비스를 제공하여 고객에게 완벽한 유연성을 제공합니다. 바로 동적 데이터 마스킹을 통한 볼트가 필요하지 않은 토큰화와 볼티드 토큰화(vaulted tokenization)입니다. 두 솔루션 모두 데이터 센터, 빅데이터 환경, 클라우드 등 상주 위치에 관계 없이 민감한 자산을 보호하고 익명화합니다.

### BYOK(Bring Your Own Key)

탈레스는 [CCKM\(Ciphertrust Cloud Key Manager\)](#)을 배포해 이 보험회사가 퍼블릭 클라우드 솔루션 제공업체의 키 볼트(key vault)에서 BYOK 접근 방식을 활용할 수 있도록 지원했습니다. 이 보험회사가 Thales CCKM을 배포한 주된 목적은 암호화 키의 소유권을 보장받는 것이었습니다. 그럼으로써 이 보험회사는 퍼블릭 클라우드 솔루션 제공업체가 전적으로 클라우드에 저장된 데이터와 협업 애플리케이션에 사용되는 데이터에 대한 암호화 키를 생성 및 저장하도록 허용하지 않을 수 있어 엄격한 감사 및 규정 준수 요건을 충족하면서도 강력한 키 관리를 달성할 수 있었습니다.

BYOK을 배포하고 2년 뒤 이 보험회사는 BYOE(Bring Your Own Keys)를 클라우드 보안 수준이 가장 높은 [BYOE\(Bring Your Own Encryption\)](#)로 마이그레이션할 수 있었습니다.



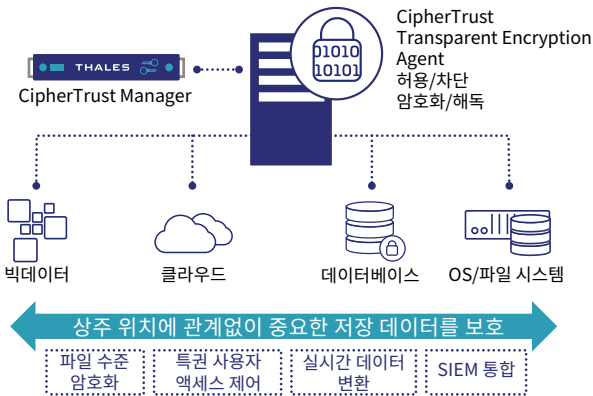


볼트가 필요 없는 토큰화는 중앙 집중식 구성을 제공하여 명확한 업무 분장을 보장합니다.

### 변화하는 환경 속에서 데이터베이스 암호화

데이터 센터의 온프레미스 데이터베이스와 파일을 보호하는 것만으로는 중요한 데이터를 보호하는 데 충분하지 않습니다. [CipherTrust Manager](#)를 배포한 탈레스는 이 보험회사의 디지털 트랜스포메이션 여정을 지원하는 동시에, 대량의 개인 데이터, 건강 관련 데이터 및 금융 데이터를 보호하기 위해 [CipherTrust Transparent Encryption](#) 사용을 제안했습니다.

#### CipherTrust Transparent Encryption



- [CipherTrust Transparent Encryption](#)은 중앙 집중식 키 관리, 특권 사용자 액세스 제어, 상세한 데이터 액세스 감사 로깅 등을 통해 저장 중인 데이터를 암호화합니다. 따라서 조직은 데이터의 상주 위치에 관계없이 데이터 보호를 위한 규정 준수 및 모범 사례 요구 사항을 충족할 수 있습니다.

뿐만 아니라 CipherTrust Transparent Encryption을 사용하면 파일, 볼륨 및 연결된 클라우드 스토리지를 보호하는 것으로 입증된 하드웨어 가속 암호화 솔루션을 사용해 암호화, 액세스 제어 및 데이터 액세스 로깅에 대한 규정 준수 및 모범 사례 요구 사항을 충족하는 동시에, 물리적/가상/클라우드 환경에서 액세스 제어 및 데이터 액세스 감사 로깅을 수행할 수 있습니다.

### 이점

#### 보안 및 규정 준수 강화

탈레스의 데이터 보호 제품 및 솔루션은 eIDAS(electronic IDentification, Authentication and Trust Services) 규정, PCI DSS(Payment Card Industry Data Security Standard), GDPR(General Data Protection Regulation), HIPAA(Health Insurance Portability and Accountability Act), FISMA(Federal Information Security Management Act) 등을 포함한 다양한 보안 및 개인정보보호 요건을 충족할 수 있도록 도와줍니다.

#### 직원 및 자원 효율성 최적화

탈레스는 연동이 가능하도록 제품을 설계하고, 글로벌 지원을 위한 단일 창구를 마련하며, 진화하는 위협으로부터 데이터를 보호한 실적을 입증하고, 최대 규모의 데이터 보안 파트너십 에코시스템을 구축함으로써 업계의 광범위한 데이터 보안 사용 사례를 지원하고 있습니다. 탈레스는 고객이 보호 기능을 신속하게 배포 및 모니터링할 수 있도록 보장하기 위해 용이성, 자동화를 위한 API, 응답형 관리에 모든 역량을 집중하고 있습니다. 또한 직원이 최소한의 시간을 들여 신속하고 안정적으로 솔루션을 구현할 수 있도록 설계, 구현 및 교육 지원에 전문 서비스 및 파트너를 투입하고 있습니다.

#### 총소유비용(TCO) 절감

탈레스의 데이터 보호 포트폴리오는 새로운 사용 사례로 손쉽게 확장이 가능하고 기존 기술과 신규 기술을 모두 보호하는 것으로 입증된 포괄적인 데이터 보안 제품 및 솔루션 세트를 제공합니다. 탈레스 솔루션을 사용하면 운영 비용과 자본 지출을 줄이는 동시에 투자 효과를 보장할 수 있습니다.

### 탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.