Discover Protect Control

Data Security for a Zero Trust World

탈레스 회사소개서

THALES
Building a future we can all trust

Thales Group 사업분야

THALES GLOBAL BUSINESS AREAS

#1
전 세계
데이터 보호 분야

#2
전 세계
민간 인공위성 시스템

#1
전 세계
항공 교통관제 시스템

#2
전 세계 기내
엔터테인먼트 시스템

#3
전 세계 상업용
항공전자 시스템

#1
유럽 시장 내
다중 기능 센서 개발

#1
전 세계
스마트 공항 분야

직원 **81,000명+**

68개 국가에서
사업 운영

연간 R&D 투자
금액 **1조 3천억원+**

2021년 매출
21조 원+

Thales Cloud Protection & Licensing

탈레스 CPL

- 데이터 보호
- 접근 관리 및 인증
- 소프트웨어 수익화

- 전 세계 180개 국가에서 30,000개 이상의 고객 보유
- 전 세계 6개 센터를 통한 기술지원 및 글로벌 서비스 제공
- 국제 규격의 보안인증 - FIPS, Common Criteria, PCI HSM
- 20개 선도적 클라우드 사업자와의 파트너십 제휴

시장을 선도하는 데이터 암호화 솔루션

#1
범용 하드웨어 보안 모듈(HSM)

#1
데이터 보호 플랫폼

#1
네트워크 암호화 장치

#1
지불 결제용 HSM

#1
키 관리 솔루션

#1
클라우드 HSM

복잡한 환경에서 데이터를 보호하는 가장 확실한 방법

Discover (검출)

- 민감 데이터의 효과적인 검출 및 분류
- 데이터 시각화를 통한 리스크 분석

Protect (보호)

- 암호화, 접근 제어, 토큰화를 통한 데이터 보호
- 도난이나 유출 시 데이터를 읽을 수 없고 쓸모없게 만드는 작업

Control (통제)

- 중앙 집중식 키 관리로 암호키 통제
- 멀티 클라우드 키 관리
- FIPS 140-2 준수

어떤 환경이든, 고객이 원하는 방식으로

PROTECT ANYTHING


Big data


Intellectual Property


Financial data

Enterprise data


Identities of Things


Payments & digital transactions

PROTECT ANYWHERE


Applications


Data centers


Containers


Networks

Virtual


Clouds

DELIVERED ANY WAY


On demand
cloud-based

Hybrid
Cloud &
on-premise

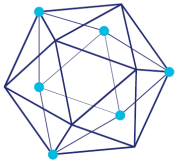

On-premise
hardware or software

정부의 디지털 전환과 혁신의 가속화

전자인증 및
전자문서 사업

멀티·하이브리드
클라우드 보안

스마트시티
IoT 인프라 보안



블록체인 프로젝트
보안

빅데이터 보안

모바일 신분증, 공공웹사이트의 민간전자서명 도입, 스마트시티 인프라 구축 등
디지털 정부혁신의 과정을 안전하고 빠르게 이끌어갑니다.

인증된 RoT(Root of Trust)를 사용하여 디지털 신분증, 어플리케이션, IoT 기기, 암호화 키를 보호

멀티·하이브리드 클라우드 내의 데이터를 **BYOK, HYOK, BYOE, 중앙 집중식 키 관리**를 통해 보호

MFA, 스마트 SSO, 중앙 액세스 제어를 통해 **제로 트러스트 모델**을 모든 환경에 도입

엔터프라이즈 기업의 모든 IT 환경에서 보안 극대화

SaaS, PaaS, IaaS
서비스 보안

온프레미스
시스템 관리

파일 repository와
각종 데이터베이스 관리

글로벌 공급망
보안

원격 IoT 기기 보안

수 많은 도입 사례에 기반한 다양한 솔루션으로
민감 데이터와 개인정보를 자동으로, 간소화하여 보호합니다.

클라우드 네이티브, 하이브리드, 온프레미스 환경에서 사용하는 모든 서드파티 보안 솔루션의 키 관리를 중앙화

조직 내부와 Salesforce, o365 등 주요 SaaS에 있는 모든 민감 정보를 **비식별화**하여 데이터 유출 **위협을 최소화**

모든 **IaaS, PaaS, SaaS, 레거시 환경**에서 **통합인증**을 통해 접근 관리를 중앙화

보안 리스크와 복잡성은 줄이고, 성장 동력을 키우는 결정

보안은 강화하고, 비용은 절감합니다.
데이터 보안의 자동화 및 간소화 실현

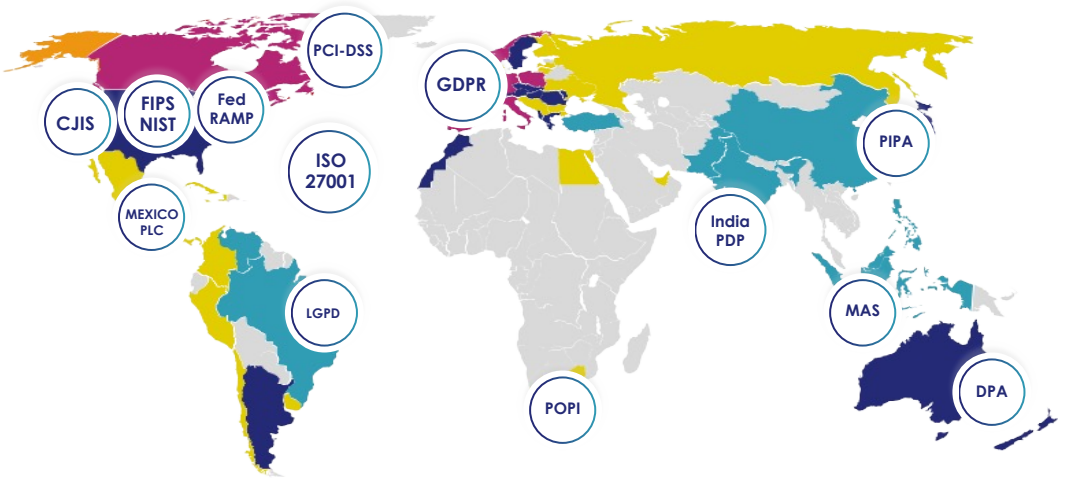
리스크와 복잡성을 제거합니다.
중앙화된 데이터 보안 거버넌스 구축으로
손쉽게 각 국가 개인정보보호법 규정 준수

디지털 트랜스포메이션을 앞당깁니다.
Security by Design의 견고한 프레임워크를
도입하여 혁신의 질과 속도를 향상

White House Cybersecurity Executive Order

European Union Cybersecurity Act

Personal Information Protection Act(PIPA)



CipherTrust Data Security Platform 살펴보기

CipherTrust Connectors

- Data Discovery and Classification
- File-level Encryption and Access Control
- Database Encryption
- Developer Crypto Tools
- Tokenization w/Dynamic Data Masking

CipherTrust Cloud Key Manager

amazon web services · Microsoft Azure · IBM Cloud · Google Cloud Platform · salesforce

High Speed Encryptor

Network encryption

CipherTrust Manager

Enterprise Key Management and Policies

Enterprise Key Management

For native encryption

Oracle
MySQL
MS Always Encrypted
IBM DB2

Powered By vmware vSAN™

vSAN/vCenter
Hadoop
Custom Apps

Full Disk Encryption
Tape Archives
NTAP, Pure, EMC, IBM, Hitachi, Dell, etc.

Luna HSM

Root of Trust

FIPS VALIDATED 140-2

Luna Cloud HSM

Root of Trust on DPoD

THALES

Use Case #1 디지털 신분증

LUNA Network HSM으로 디지털 신분증 발급 및 검증을 위한 DID 인증과정 지원

Challenge

- 디지털 신분증은 블록체인을 기반으로 하는 탈중앙화된 (decentralized) **디지털 신원증명 체계(DID, Decentralized IDentity) 기술**을 적용한다.
- 정부가 발급하여 공신력을 부여하되, 온라인 상에서 디지털 신분증 사용 및 검증에 타인 또는 기관이 개입할 수 없도록 함으로써 사생활 침해 및 감시사회 우려를 해소했다.
- 탈중앙화의 핵심 기술인 블록체인 기술에는 분산을 위해 사용될 **개인키/ 공개키 쌍의 생성 및 보호, 안전한 서명의 수행이** 요구된다.

Solution

- **Thales Luna Hardware Security Modules (HSMs)**은 정부의 루트 서명 키를 제어하고 보호하기 위해 배포되었다.
- Luna HSM은 **FIPS 140-2 레벨 3** 및 **Common Criteria** 표준에 대한 검증을 통해 **한국 정부의 엄격한 하드웨어 보안 표준 및 사양을 충족**한다.

Results

- 개인이 디지털 신분증을 통해 온라인에서 본인확인 요청을 할 경우 서비스 제공자는 해당 신분증이 실제로 발급된 것인지 발급이력만 확인 수 있다.
- 신원이 분산 관리되는 만큼 개인정보 노출 위험 역시 줄어들게 되는데, 이때 사용되는 블록체인의 **서명을 안전한 환경에서 수행**하고, 서명에 필요한 키를 **신뢰할 수 있는 하드웨어 내에 보관**하여 보안성을 높일 수 있다.

THALES

Use Case #2 천안시청

CipherTrust Transparent Encryption을 활용하여 시민의 개인정보 보안 강화

Challenge

- 천안시청은 코로나 19 발발 이후 재난 지원금 신청을 위해 시스템을 신규 구축해야 했다.
- 재난 지원금 신청 시스템에는 주민등록번호, 주소, 전화번호 등 **시민들의 민감 정보**가 담겨있기 때문에 이를 보호할 수 있는 암호화 솔루션을 필요로 했다.
- 예상치 못한 천재지변 탓에 촉박한 일정 내에 시스템을 안정적으로 구축할 수 있는 솔루션을 선택하고자 했다.
- 특히 **암호화 솔루션의 속도, 안정성**, 얼마나 **다양한 파일을 안정적**으로 보호하는지를 중점적으로 검토했다.

Solution

- 암호화 솔루션은 일반적으로 연산에 덧씌워서 연산을 추가하는 방식으로 이루어지기에 속도에 대한 이슈가 가장 크며, 암호화 후 메타데이터가 바뀌어 데이터베이스나 앱에서 읽을 수 없어 수정해야 하는 방법이 대부분이다.
- 탈레스의 **CipherTrust Transparent Data Encryption** 솔루션은 기존 환경에서 동일하게 암, 복호화 기능을 수행할 수 있는 우수한 성능을 제공한다.

Results

- 천안시청은 탈레스의 CipherTrust Transparent Data Encryption를 활용해 **짧은 시일내에 시민들의 민간 정보 암호화 구축에 성공**했다.
- 천안 시청은 이어서 천안시민들의 개인정보 보안 강화를 위해 현재 구축한 홈페이지 서버 이외에 개인정보 보호에 대한 확대 프로젝트를 고려 중이다.

THALES

Use Case #3 유럽의 글로벌 자동차 제조사

CipherTrust Cloud Key Manager로 복잡한 하이브리드 IT 인프라 내 데이터 보호

Challenge

- 글로벌 자회사들이 동시에 사용하고 있는 **MS Office 365**와 **세일즈포스** 상의 민감 데이터가 보안에 취약한 상황이었다.
- **Windows, Linux, HP UX**를 포함한 여러 레거시 시스템에 저장된 민감 데이터 관련하여 다양한 규정을 준수해야 했다.
- 수십만 명의 직원들이 사용하는 내부 리소스에 대해 더 나은 **액세스 제어 방안**이 필요했다.

Solution

- **CipherTrust Cloud Key Manager (CCKM)**를 통해 Office 365와 세일즈포스의 중앙 집중식 키 관리를 수행한다.
- 복잡한 환경에서 데이터를 보호할 수 있도록 **CipherTrust Transparent Encryption**을 중앙집중식 키 관리 및 KMIP 커넥터와 함께 도입했다.
- **Luna HSM root-of-trust** 을 도입하여 **PKI 기반 엑세스 관리 및 인증** 을 구현했다.

Results

- 중앙 집중식 키 관리로 **클라우드 SaaS 환경에서의 보안을 향상**하여 데이터를 더 안전하게 보호하고 클라우드 서비스의 이점을 충분히 활용할 수 있게 되었다.
- 단일 창에서 **세분화된 보안 정책**을 시행할 수 있게 되어 **규정 준수**의 속도를 높였다.
- 수많은 직원들이 사용하는 조직 내부의 민감 데이터에 대해 **강력한 PKI 기반 액세스 관리 및 인증의 도입**으로 데이터를 안전하게 보호한다.

THALES

Use Case #4 아시아의 주요 금융그룹

CipherTrust Cloud Key Manager와 Cloud HSM 도입으로 안전한 디지털 전환 가속화

Challenge

- 디지털 트랜스포메이션 프로젝트 진행을 위해 **하이브리드/멀티 클라우드 환경에서 데이터를 보호**하고 **키를 관리**할 수 있는 확장성 있는 솔루션을 필요로 했다.
- 고객의 **개인정보, 금융정보**와 더불어 보험서비스로 인한 **건강 정보**까지 안전하게 보호하는 것이 최우선이었다.
- 클라우드로 데이터를 이전하면서 **여러 나라의 민감정보 관련 규정을 모두 준수**하고 고객에게 안전한 서비스를 제공하는 것이 목표였다.

Solution

- **Luna Cloud HSM**과 **CipherTrust Manager**를 도입하여 데이터 암호화에 사용된 키를 클라우드 상에서 안전하게 보관 및 관리할 수 있게 되었다.
- **CipherTrust Tokenization**을 통한 Vaultless 토큰화 솔루션으로 온프레미스에 저장되어 있던 데이터를 클라우드로 안전하게 이전하였다.
- **CipherTrust Cloud Key Manager** 또한 도입하여 퍼블릭 클라우드가 제공하는 암호화 키 대신 직접 키를 생성하고 관리하는 오너십을 유지할 수 있었다.

Results

- 해당 금융그룹은 FIPS140-2 레벨 3에 해당하는 암호화 솔루션을 갖추면서 여러 **보안 규정을 준수**할 수 있었다.
- 인가받은 엔터티에서만 키를 사용할 수 있도록 **업무를 분리**하고 **암호키를 완전히 제어**하여 보안이 향상되었다.
- 데이터 보안 정책에 대한 **완벽한 가시성** 및 **키 순환 자동화**로 보안 관리를 최적화했다.

THALES

Use Case #5 스마트 계량기

스마트 계량기의 인증을 위해 LUNA Network HSM으로 키 및 서명 보호

Challenge

- 공공 분야의 **자원 사용량 검침을 자동화**하고,소비자에게 사용요금을 안내하기 위해, **인증과정**에서 발생할 수 있는 공격을 **차단**할 수 있어야 했다.
- 이때 개인정보와 자원 사용량등의 민감한 데이터를 보호해야 하는데, 이를 위해 **인증을 위한 키를 안전하게 보호**하며 서명을 수행할 수 있는 **신뢰할 수 있는 보안 환경**과 데이터 암호화를 위한 키 보호 및 **안전한 암호화 환경**이 요구되었다.

Solution

- **Thales Luna Hardware Security Modules (HSMs)** 을 통해 사용량 검침을 위한 기기 인증및 사용자 인증에 필요한 키 보호와 사용량 암호화를 위해 배포된다.
- Luna HSM은 **FIPS 140-2 레벨 3** 및 **Common Criteria** 표준에 대한 검증을 통해 **한국 정부의 엄격한 하드웨어 보안 표준 및 사양을 충족**한다.
- **KeySecure 와 ProtectApp** 을 통해 서명에 필요한 키를 관리하고, Application data를 보호한다.

Results

- 가입자의 개인정보와 스마트 계량기에서 수집된 자원 사용량에 대한 데이터를 보호하기 위해 HSM 과 KeySecure를 통해 **암호화키와 서명에 필요한 키쌍을 안전하게 생성할** 수 있게 되었다.
- 신뢰할 수 있는 환경에서 **효과적인 키관리와 데이터 암호화를 보장**하게 되었다.

THALES

Trusted by the most recognized brands in the world

FINANCE

BARCLAYS

UBS

JPMORGAN CHASE & CO.

Deutsche Bank

TECHNOLOGY

Microsoft

salesforce

Verifone

HEALTHCARE

CVS pharmacy

McKESSON

DELTA DENTAL

MOLINA HEALTHCARE

PAYMENTS

VISA

DISCOVER

AMERICAN EXPRESS

GOVERNMENT

Australian Government
Department of Defence

Ministry of Defence

UNITED STATES POSTAL SERVICE

SERVICE PROVIDERS

FUJITSU

orange Business Services

AT&T

rackspace technology.

RETAIL

Walmart

Office DEPOT OfficeMax

GAP

WILLIAMS SONOMA

MANUFACTURING

SAMSUNG

Kellogg's

BOSCH

3M

MICHELIN


THALES
Building a future we can all trust