THALES
Building a future we can all trust

클라우드에서의 민감 데이터 관리

Using Thales CipherTrust Data Security Platform

2023. 05. 19

조재웅 부장Jaewoong.Cho@thalesgroup.com

목차

THALES
Building a future we can all trust

GLOBAL EDITION

2023 DATA THREAT REPORT

Perspectives and Pathways to Digital Sovereignty and Transformation

#2023DataThreatReport
cpl.thalesgroup.com

We're only human:

55%(KR 56%)

최근 클라우드 데이터 유출을 경험한 응답자가 꼽은 클라우드 데이터 유출의 근본 원인 **1위**

사람의 실수

IAM(Identity and Access Management)
데이터 유출에 대한 최고의 완화 조치

28%

응답자의 28%는 IAM을 사이버 공격으로부터 민감한 데이터를 보호하는 데 가장 효과적인 최고의 보안 기술로 꼽았습니다.

강력한 MFA 채택률이 65%로 증가

65%
(KR57%)

: U V AE7 QH 1N 18/13SF5XP
J^ X I L:X# D21DL31WV6G<K
X {S OEB 3UV S AL 58=2Q43

개선된 내부 보안인식, 하지만 뒤쳐지는 보안성과

81%
(KR 76%)

자사의 시스템에서 관리되는 개인정보가 안전하다고 확신

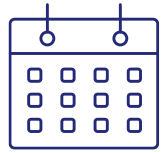
49%
(KR 53%)

랜섬웨어 공격이 증가하고 있다고 응답.

51%
(KR 47%)

공식적인 랜섬웨어 방어계획이 없음

37%
(KR 34%)



지난 12개월 안에 보안 침해 사고가 발생

22%

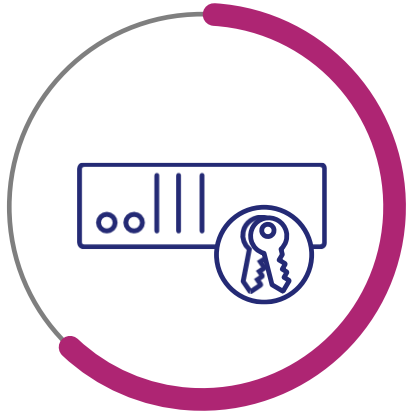
지난 12개월안에 랜섬웨어 공격을 경험

Digital sovereignty is...

새로운 전략적 이니셔티브로 부상하고 있으며,
개인정보 보호 규정 준수는 기업이 디지털 혁신을 가속화할 수 있는 기회

96% (KR 97%)

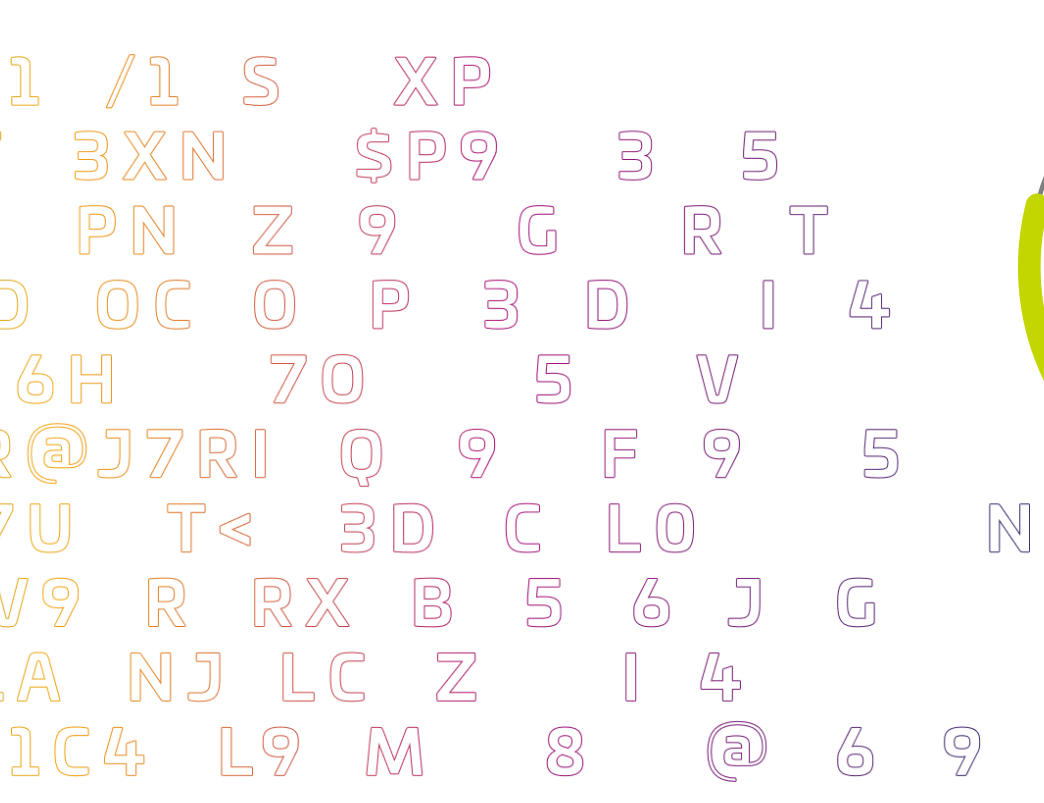
다양한 수준의 **디지털 주권**을 달성하기 위해 **데이터의 위치와 관할권을 지정 또는 변경하거나 전체 데이터 암호화**를 허용가능한 조치로 간주



62% (KR 59%)

데이터 제어의 복잡성을 가중시키는 최소 5개의 엔터프라이즈 키 관리 시스템을 사용

현실이 된 멀티 클라우드, regardless of cloud maturity.



79%

업무를 위해 운영중인 **퍼블릭 클라우드를 두 개 이상 보유**하고 있으며, 이는 2022년에 보고된 57%보다 **훨씬 높은 수치**입니다.

클라우드 도입을 따라잡는 클라우드 리스크 인식

38%
(KR 47%)

SaaS apps 을 사이버 공격의 가장 큰 타겟을 인식

36%
(KR 27%)

cloud-based storage 을 사이버 공격의 가장 큰 타겟으로 인식

77%

5G에 대한 보안 우려.

75%
(KR 77%)

5G 네트워크에 연결되는 사람과 장치의 신원을 보호하는 것을 가장 큰 우려사항으로 선택

: U V AE7 QH 1N 18/13SF5XPH
J^ X I L:X# D21DL31WV6G<KN

변화하는 규제 환경 및 외부 이벤트, 데이터 보안 대응력이 필요

83%

데이터 주권 및/또는 개인 정보 보호 규정이 조직의 클라우드 구축 계획에 영향을 미칠 것을 매우 또는 다소 우려

55%

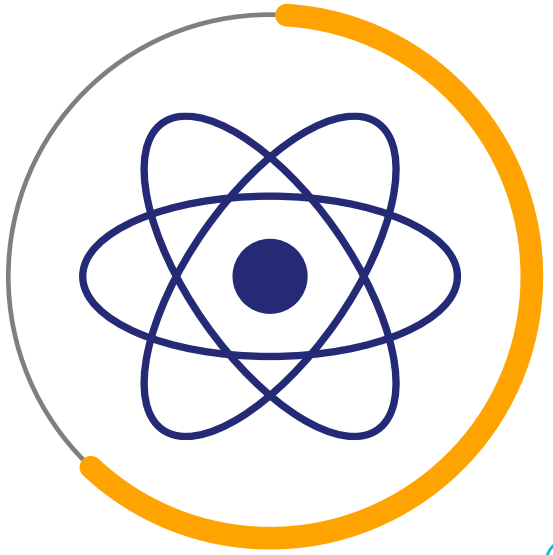
조직 내의 사내 네트워크보다 클라우드(클라우드/하이브리드) 환경에서 개인 정보 보호 및 데이터 보호 규정을 관리하는 것이 더 복잡하다는 데 동의하거나 강하게 동의

현실로 다가오는 양자 암호화

Only...

49%

49%의 응답자만이 **공식적인 랜섬웨어 대응책** 마련



62% (KR 52%)

Network decryption 이 가장 큰 보안의 위협으로 응답

THALES
Building a future we can all trust

Sponsored by

EXCLUSIVE NETWORKS

Visit **cpl.thalesgroup.com/data-threat-report** to download the full report

S&P Global
Market Intelligence

Source: 2023 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

분석가의 조언, 데이터 보안 향상을 위한 플랫폼 방식 접근

Successful security and risk management leaders can significantly improve business utilization and data value by building a migration plan from siloed data security offerings to data security platforms.

Gartner 2022
Strategic Roadmap for Data Security Platform Convergence

The Gartner Approach

THALES

탈레스가 제안하는 데이터 보안을 위한 통합적 접근 방식

DISCOVER

검출

민감 데이터의 검출 및 분류

PROTECT

보호

암호화 또는 토큰화를 통한 데이터 보호

CONTROL

통제

보호 중인 데이터에 대한 접근 통제 및
암호 키와 보호 정책의 중앙 집중적 관리

THALES

CipherTrust Data Security Platform - CDSP

CipherTrust Manager

암호 키 및 정책의 중앙 관리

CipherTrust Connectors

- Discovery and Classification
- Ransomware Protection, Encryption and Access Control
- Database Protection
- Application Data Protection
- Tokenization
- Enterprise
- Multi Cloud
- Secrets Management

Discovery

Encryption and tokenization

Key management

THALES

CipherTrust Manager : 플랫폼의 중심 솔루션

CipherTrust Manager

- 중앙 집중적 키 관리
- 역할 기반 통제
- 향상된 감사 및 보고서 기능
- 개발자 친화적 REST APIs
- 멀티 테넌트
- FIPS 140-2 인증

THALES

민감 데이터의 검출 및 분류

성공적인 암호화 전략을 방해하는 **첫번째 장벽** –
조직에서 중요 데이터가 저장된 위치 찾기

위치에 제약없이 모든
유형의 민감한 데이터 찾기 #1

리스크 분석 및 보고 #2

적극적인 보호 #3

CipherTrust Data Discovery and Classification

DISCOVER

THALES

위치에 제약 없는 민감 데이터 보호

Where 보호 계층	How CipherTrust 커넥터		
네트워크	Data Protection Gateway for REST	Tokenization (Vaultless & Vaulted)	
어플리케이션	Application Data Protection (SDKs)		
데이터베이스	Database Protection	Application Key Management (for native TDE)	Batch Data Transformation
파일 시스템	Transparent Encryption with Live Data Transformation	Transparent Encryption solutions for: - Amazon S3 - SAP HANA - Kubernetes - Teradata	

보안 요구 사항 및 인프라에 맞는 기술 스택의 각 계층에 대한 솔루션 제공

파일 시스템 계층에서의 데이터 보호

민감 데이터가 어디에 있든 보호하여 최소한의 중단, 노력 및 비용으로 규정 준수 요건을 충족

Transparent Encryption

인프라, 애플리케이션 또는 워크플로를 변경하지 않고 데이터를 암호화하고 권한 있는 사용자 액세스 제어를 정의

Live Data Transformation

다운타임 없는 암호화 적용 및 무중단 키 교체

Advanced data protection solution integrations

Windows, aws, Kubernetes, hadoop, Red Hat Enterprise Linux, SUSE, teradata., ORACLE, Ubuntu, UNIX, Microsoft SQL Server, SAP HANA

...and more

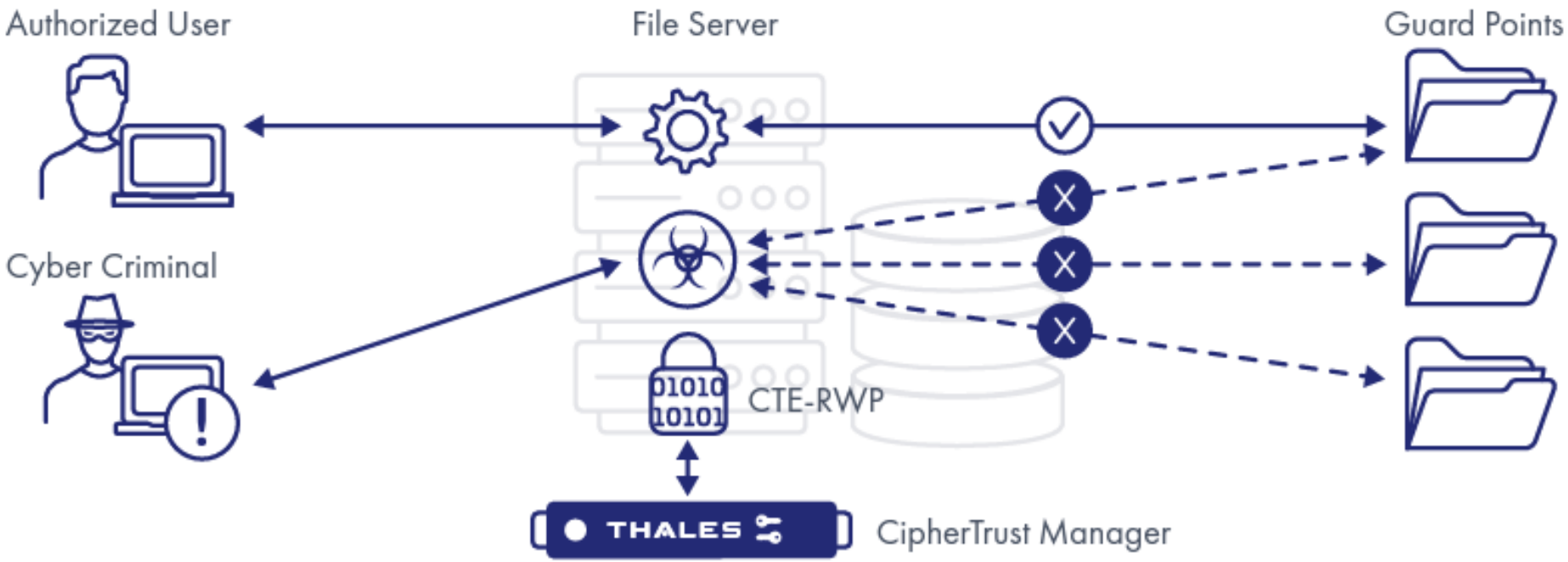
CTE-RWP: CipherTrust Transparent Encryption – Ransomware Protection

랜섬웨어 공격에 대한 다각적 방어 강화

1. 보호 영역에서 모든 파일 입출력을 감지하여 악성 활동에 대한 경고 또는 차단
2. 랜섬웨어로 식별되는 활동 탐지 (과도한 데이터 접근 또는 유출, 무단 암호화 등 악의적 동작)
3. 알려진 랜섬웨어 파일 서명 데이터베이스에 의존하지 않고 활성 프로세스를 모니터링
4. 랜섬웨어가 CTE-RWP 이전에 설치된 경우에도 랜섬웨어 방어
5. 통합 데이터 보안 관리를 간소화하는 CDSP 콘솔(CM)을 공유

THALES

Enhance security posture by detecting malicious activities to block Ransomware attacks



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

DevSecOps에서의 마찰 감소

속도를 유지하면서 데이터 보호 컨트롤을 애플리케이션에 배포

CipherTrust Connectors

Transparent Encryption for Kubernetes (CTE-K8s)

Data Protection Gateway for REST (DPG)

Orchestration

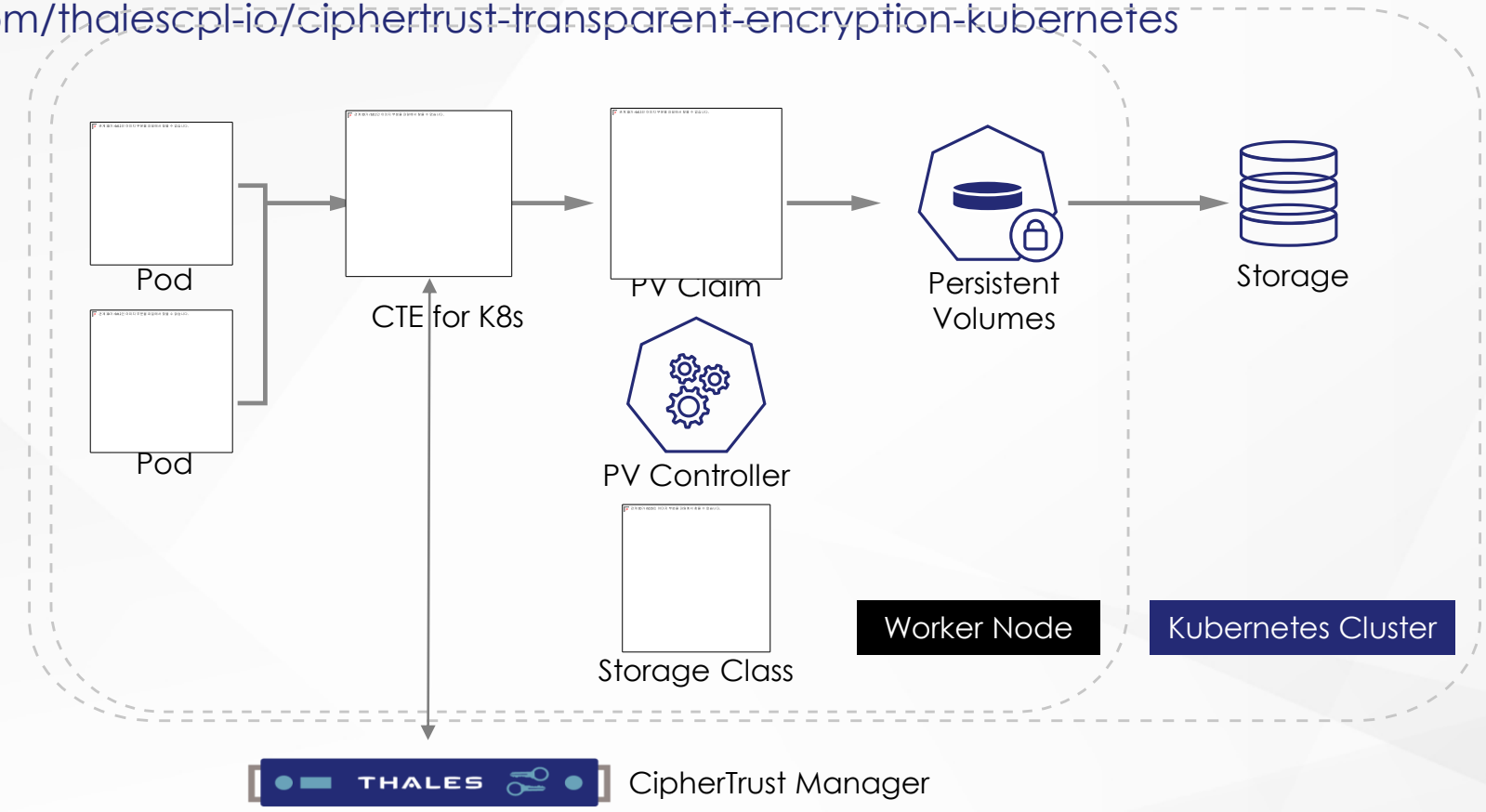
- Helm
- Ansible
- Terraform
- Power Shell

Monitoring

- SIEM Compatible Logging
- Readiness Probes

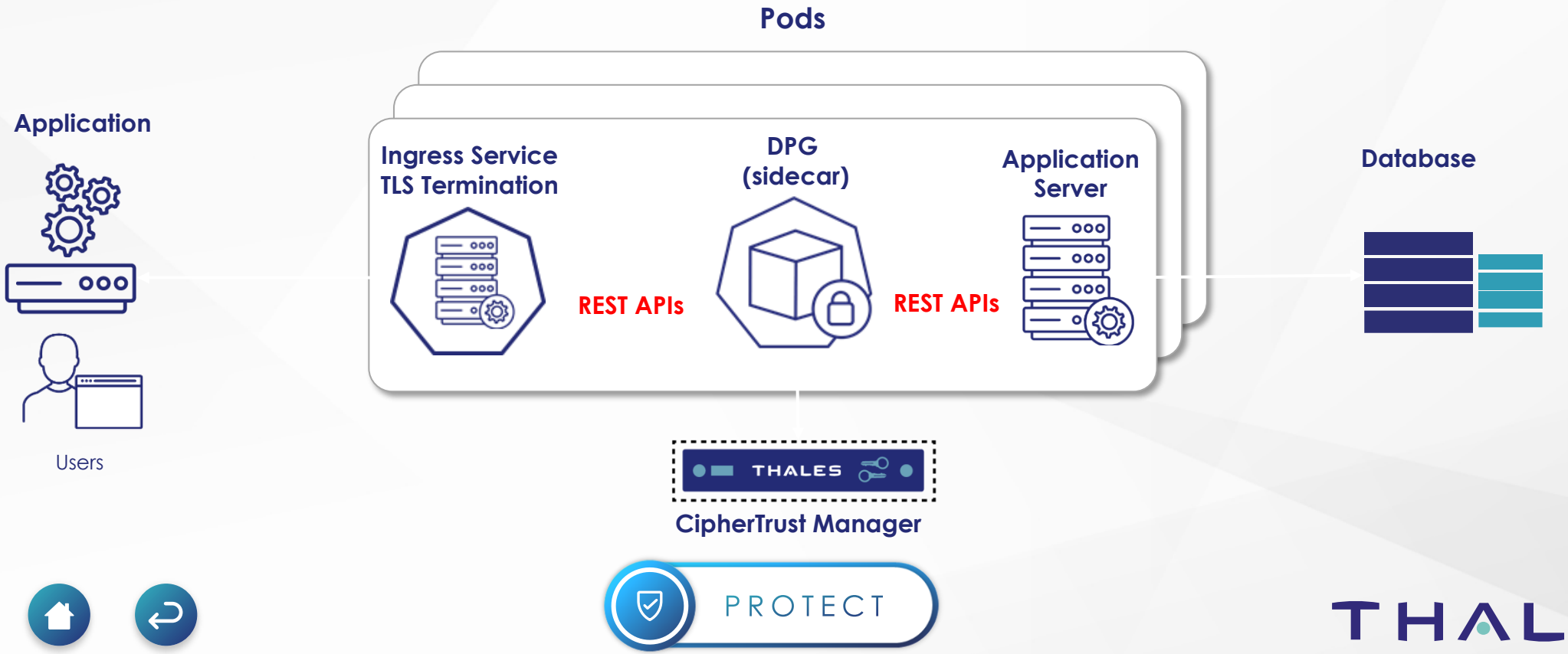
CTE-K8s

- Kubernetes 툴과의 연동을 통해 컨테이너 환경에서 투명한 파일 암호화 제공
- 도커 컨테이너 이미지 형태로 제공
  - https://github.com/thalescpl-io/ciphertrust-transparent-encryption-kubernetes



DPG

- Micro Service Architecture 상에서 어플리케이션 수정 없이 투명한 암호화 제공
- K8s POD 이미지 형태로 제공
  - https://hub.docker.com/r/thalesciphertrust/ciphertrust-data-protection-gateway
  - https://github.com/snpranav/data-encryption-in-transit-demo



PROTECT

DevSecOps를 위한 secret 관리

대규모 secret 보호

CipherTrust Secrets Management*

Automate access to

- Secrets
- Credentials
- Certificates
- API keys
- Tokens

- 다양한 타입의 시크릿에 대한 중앙 관리
- DevSecOps를 위한 손쉬운 사용법
- 하이브리드 또는 멀티 클라우드 환경을 위한 SaaS (Software as a Service) 확장성 제공

Automate processes for

- Creating
- Storing
- Rotating
- removing

*Powered by Akeyless Vault

기업 전반의 중앙화된 키 관리

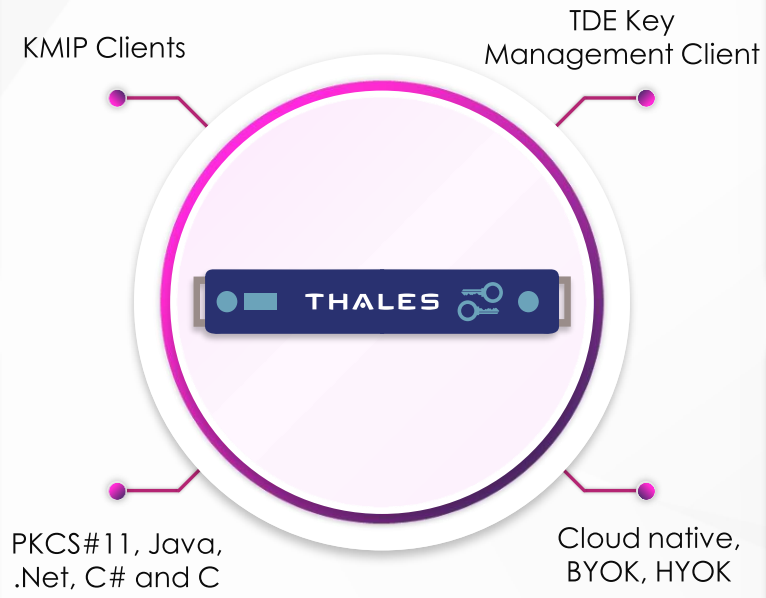
주요 엔터프라이즈 스토리지 및 서버, 데이터베이스,
클라우드, SaaS 벤더와의 광범위한 파트너 통합

Data storage vendors, big data

PURESTORAGE
NUTANIX
vmware READY vSAN
mongoDB.
Hewlett Packard Enterprise
IBM
DELL EMC
NetApp

Home-grown apps, web servers

Microsoft
HashiCorp
NGINX
APACHE SOFTWARE FOUNDATION
ORACLE



Database (TDE) Key Management

ORACLE EXADATA
Microsoft SQL Server
ORACLE

Cloud Key Management

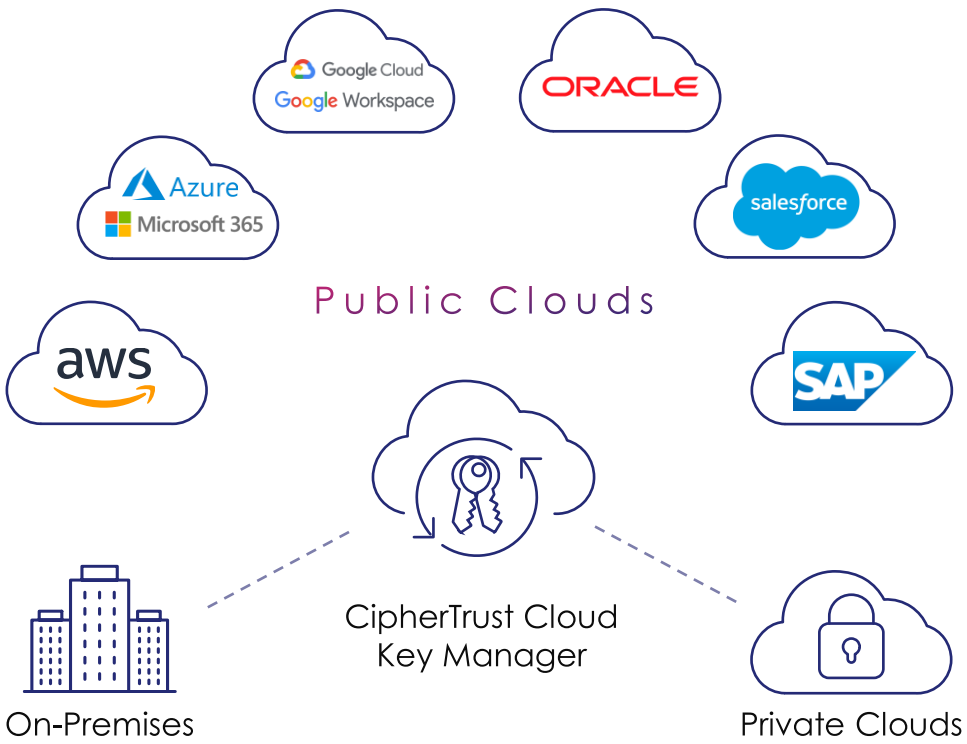
Azure
Microsoft 365
Google Cloud
Google Workspace
aws
ORACLE
SAP
salesforce

CONTROL

THALES

클라우드 전반에서 중요 데이터에 대한 제어

데이터와 클라우드 공급자 간의 의무 분리를 통해
데이터 보안 및 개인 정보 위험 완화



- 단일 UI로 클라우드와 온프레미스의 모든 조합에서 BYOK, HYOK 및 클라우드 네이티브 암호화 키에 대한 다중 클라우드 키 관리를 중앙 집중화
- 지역 전체에 걸친 단일 창 보기 및 공통 API 세트로 자동화된 키 수명 주기 관리를 통해 효율성 향상
- 데이터 주권법 및 개인정보 보호 규정 준수 입증

데이터 센터와 하이브리드 환경을 위한 CDSP 적용 옵션

Virtual CipherTrust
FIPS Level 1
-or-
Luna or Cloud HSM RoT


Cloud


On-Premises

Virtual

Physical CipherTrust
FIPS Level 1
-or-
Luna or Cloud HSM RoT

Physical CipherTrust
FIPS Level 3
Luna PCI-HSM onboard


On-Premises

Physical

Virtual CipherTrust

Clustered

Physical CipherTrust

Hybrid

THALES

필요한 곳에서 원하는 방식으로 제공되는 보안

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-premises hardware or software
- Hybrid cloud & on-premises
- As a service

THALES

Customer Case - Leading Indian Bank

Rehost
Lift and Shift

고객의 요구

신규 고객을 **원격으로 등록**하여 캡처한 **CRM 및 비정형 EKYC 데이터**를 포함하여 **60개의 SQL DB를 Azure로 마이그레이션**

Thales 솔루션

CipherTrust Cloud Key Manager and **Transparent Encryption (BYOE)** of **PII** and **sensitive data** to meet industry compliance

결과

Cost reduction

increased efficiency

Time to Value **6 Months**
> 100% ROI 3 Years

THALES

Customer Case - Industrial Manufacturer

Replace
SaaS

고객의 요구

원격 근무 인력이 사용하는 **협업 툴**에 저장된 **민감 데이터 및 PII 보호**

Thales 솔루션

CipherTrust encryption and **external key management** to **encrypt data** stored on client side outside of cloud

결과

Documents containing **sensitive data** are **encrypted inside Google Chrome browser** so Google is **not able to see data in clear; regulation requirements.** This solution was customer built and is fully cloud native

THALES

Customer Case - Leading Korean OTT Service Provider

Cloud Native
By design

고객의 요구

다양한 개발 언어 환경에 분산되어 있는 암호 키 통합 관리

서비스 별로 독자적으로 개발된 암호화 방식의 표준화

Thales 솔루션

PoC를 통한 사전 검증

Virtual CipherTrust Manager – RESTful API for Key management and Encryption

결과

사용 중인 클라우드 환경에 최적화된 통합 암호 키 관리를 통해 **보안 요건 준수**

표준화된 암호화 관리

THALES