

# 퍼블릭 클라우드에서의 민감 데이터 관리

- 탈레스 클라우드 보안 연구 공유
- 탈레스의 데이터 보호 전략

Thales CPL 구병춘 이사

[cpl.thalesgroup.com](http://cpl.thalesgroup.com)

# Agenda

2022 탈레스 클라우드 보안 연구

탈레스의 데이터 보호 전략





APAC Edition

**THALES**  
Building a future we can all trust

# 2022 탈레스 클라우드 보안 연구

#2022CloudSecurityStudy

---

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

---

# 클라우드 환경으로 전환 중인 APAC 지역 기업

애플리케이션의 클라우드 마이그레이션을 위해 아래 방식 적용:

22%

리프트 앤 시프트 방식

16%

클라우드 및 PaaS용으로 앱을 재설계  
또는 리팩토링

33%

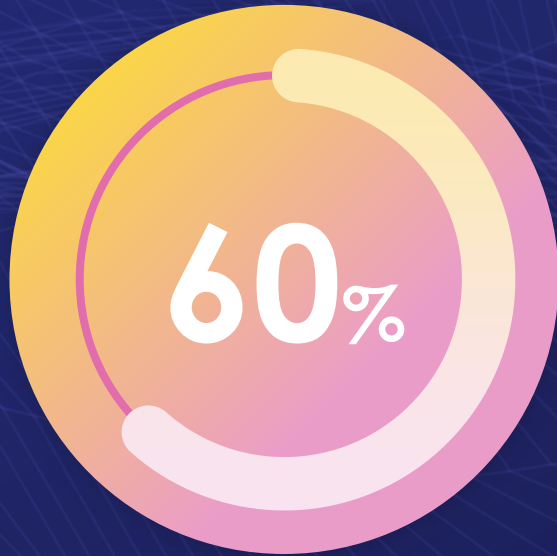
재구매 및 마이그레이션

23%

리프트 앤 시프트 방식과 재설계 방식을  
분할해서 적용



# 멀티클라우드 사용의 증가...



**SaaS, IaaS 및 PaaS 클라우드  
플랫폼을 혼용하고 있다고 응답**

응답자의 60%가 클라우드(SaaS/IaaS/PaaS)  
제공업체를 한 곳 이상 이용하고 있다고 응답

# 클라우드 복잡성이 주요 관심사로 부상



49%

응답자의 49%가 온프레미스 네트워크보다 클라우드가 개인정보보호 및 데이터 보호 규정을 관리하기 더 복잡하다는 데 동의



Only 19%

단지 19%의 응답자가 민감 데이터의 60% 이상을 외부 클라우드 제공업체에 저장하고 있다고 보고



# 감사 실패 및 데이터 유출 그리고 클라우드 데이터 유출

4%

전년 대비 4% 낮은 수의 응답자가 작년에 클라우드에 저장된 데이터와 애플리케이션에서 데이터 유출 및 감사 실패를 경험했다고 응답

2021

37%



33%

2022

# 감사 실패 및 데이터 유출 그리고 클라우드 데이터 유출



43%

설문 조사에 응한 APAC 지역 기업의  
43%가 최근 12개월 내에 감사 실패를  
겪었다고 응답



50%

APAC 지역 기업의 50%가 특정  
시점에 데이터 유출을 겪었다고  
응답



# 감사 실패 및 데이터 유출 그리고 클라우드 데이터 유출

지난 1년 동안 데이터 유출을 경험한 응답자 수 감소

2021

39%



32%

2022

# 클라우드 보안 정책 및 표준

클라우드 보안 정책과 표준 및 적용에 관한 질문에 다음과 같이 응답:



**47%**

정책을 보안 팀이 중앙에서 정의하고 있으며, 기술 표준의 정의 및 정책 적용은 클라우드 제공 팀이 담당하고 있다고 응답



**38%**

보안 팀이 원하는 도구를 사용하여 정책과 표준을 중앙에서 정의 및 적용한다고 응답



**15%**

정책, 표준 및 적용을 클라우드 제공 팀에 맡기고 있다고 응답



# 클라우드 환경의 암호화



38%

"세이프 하버" 조항 덕분에 필수 의무가 된  
데이터 유출 알림 프로세스 회피

46%

내부에서 결정하는 보안 아키텍처가  
클라우드에서 암호화가 사용되는 위치와  
방식을 결정하는 주요 동인이라고 답

Only 21%

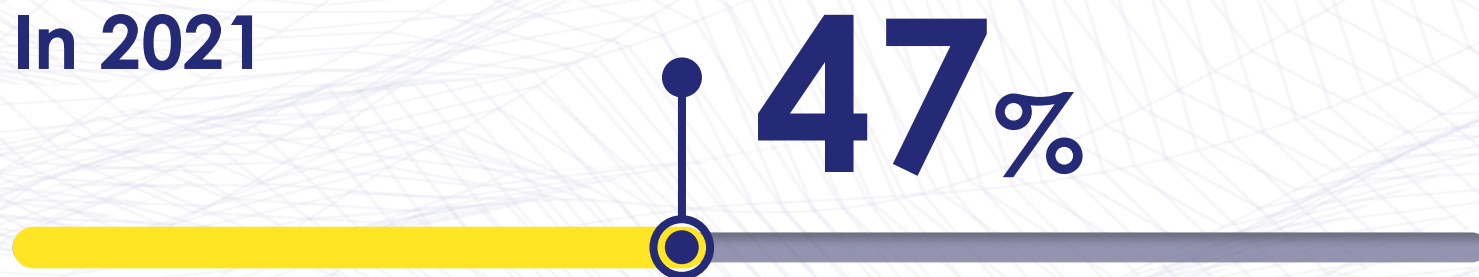
클라우드에 저장된 중요한 데이터의 60% 이상을  
암호화하고 있다고 답한 응답자는 21%에 불과

# 암호 키 관리

클라우드 콘솔에서 키를 관리하는 비율이 올해는 7% 증가



In 2021



In 2022





# 암호 키 관리

키 관리 시 다수의 솔루션으로 분산되는 현상이 문제라고 응답



**12%**

1~2개의 키 관리 솔루션 사용



**33%**

3~4개의 키 관리 솔루션 사용



**55%**

5개 이상의 키 관리 솔루션 사용

# 제로 트러스트



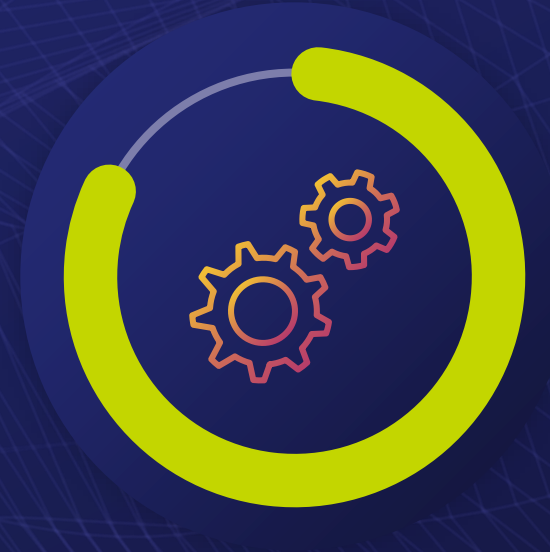
20%

제로 트러스트 전략을 아직  
마련하지 않았다고 응답



62%

클라우드 액세스에서 제로 트러스트  
원칙과 기술을 활용할 것으로  
기대한다고 응답



80%

제로 트러스트 계획을 고려  
중이거나, 평가 중이거나, 실행  
중이라고 응답



451 Research

**S&P Global**

Market Intelligence

**[cpl.thalesgroup.com/apac-cloud-security-research](https://cpl.thalesgroup.com/apac-cloud-security-research)**

451리서치의 권고 사항이 포함된 전체 연구보고서 다운로드

Source: 2022 Cloud Security custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

# 탈레스의 데이터 보호 전략



# 탈레스의 데이터 보호 전략

THALES  
Building a future we can all trust



검출: 모든 데이터에 대한 검출 및 등급화



보호: 저장, 이동, 사용 중인 민감 데이터 보호



통제: 민감 데이터에 대한 사용자 접근 통제 및  
생애 주기 전반의 키 관리



# CipherTrust Manager Community Edition

탈레스의 민감 데이터 보호 및 키 관리 제품 CM의 **free-forever** 버전  
아래 2개의 full enterprise-edition 데이터 보호 제품 라이선스 기본 제공

- CipherTrust Data Protection Gateway (DPG)
- CipherTrust Transparent Encryption for Kubernetes (CTE for K8s)

제품 소개 및 다운로드 링크: <https://ciphertrust.io/>



CipherTrust Manager  
Community Edition



CipherTrust Data  
Protection Gateway



CipherTrust Transparent Encryption  
for Kubernetes

CipherTrust Connectors

*Try the solution with zero paperwork and no expiration date – at no charge*



# CM CE – Enterprise 버전과의 기능 비교

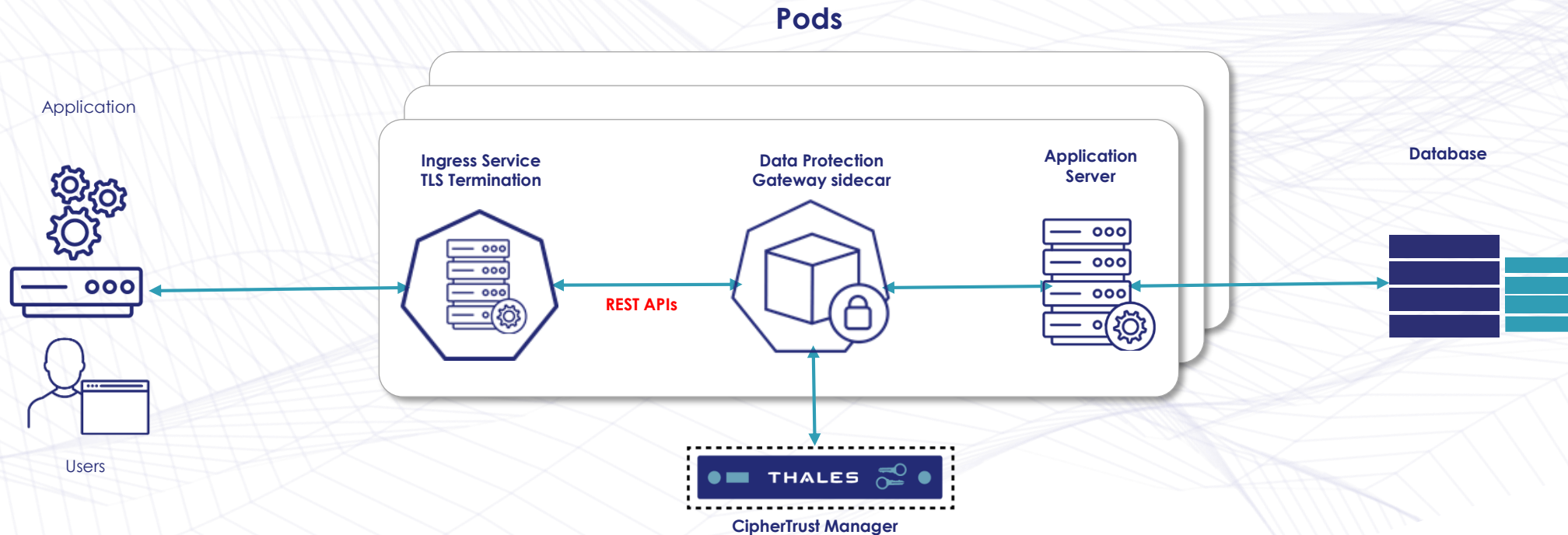
FEATURES	CipherTrust Platform Products	Community Edition	Enterprise Edition
Key Management REST APIs	CM	✓	✓
Encryption and Data Protection REST APIs	CM	✓	✓
Identity Providers Integrated	CM	Local Users only	Local, LDAP/AD, OIDC
Clustering	CM		✓
Multi-domain Support (Separation of duties)	CM		✓
Built-in or External Network HSM (FIPS 140-2, L3 Certified)	Luna Network HSM		✓
CipherTrust Connectors			
Transparent Application Protection	DPG	✓	✓
Transparent Encryption for Kubernetes Environments	CTE-Kubernetes	✓	✓
Cloud Key Management	CCKM		✓
Data Discovery and Classification	DDC		✓
Transparent Encryption for Files/Folders	CTE		✓
Database Protection	CDP		✓
Application-level Data Protection	CADP		✓
Tokenization – Vaulted, Vaultless	CT-V, CT-VL		✓
Batch Data Transformation	CBDT		✓

# DPG – Data Protection Gateway

도커 컨테이너 이미지 형태로 제공

Micro Service Architecture 상에서 어플리케이션 수정이 불필요한 투명한 암호화  
내부적으로 RESTful API 콜을 통해 동작

CM CE와의 연동을 통해 3개의 DPG 라이선스 제공





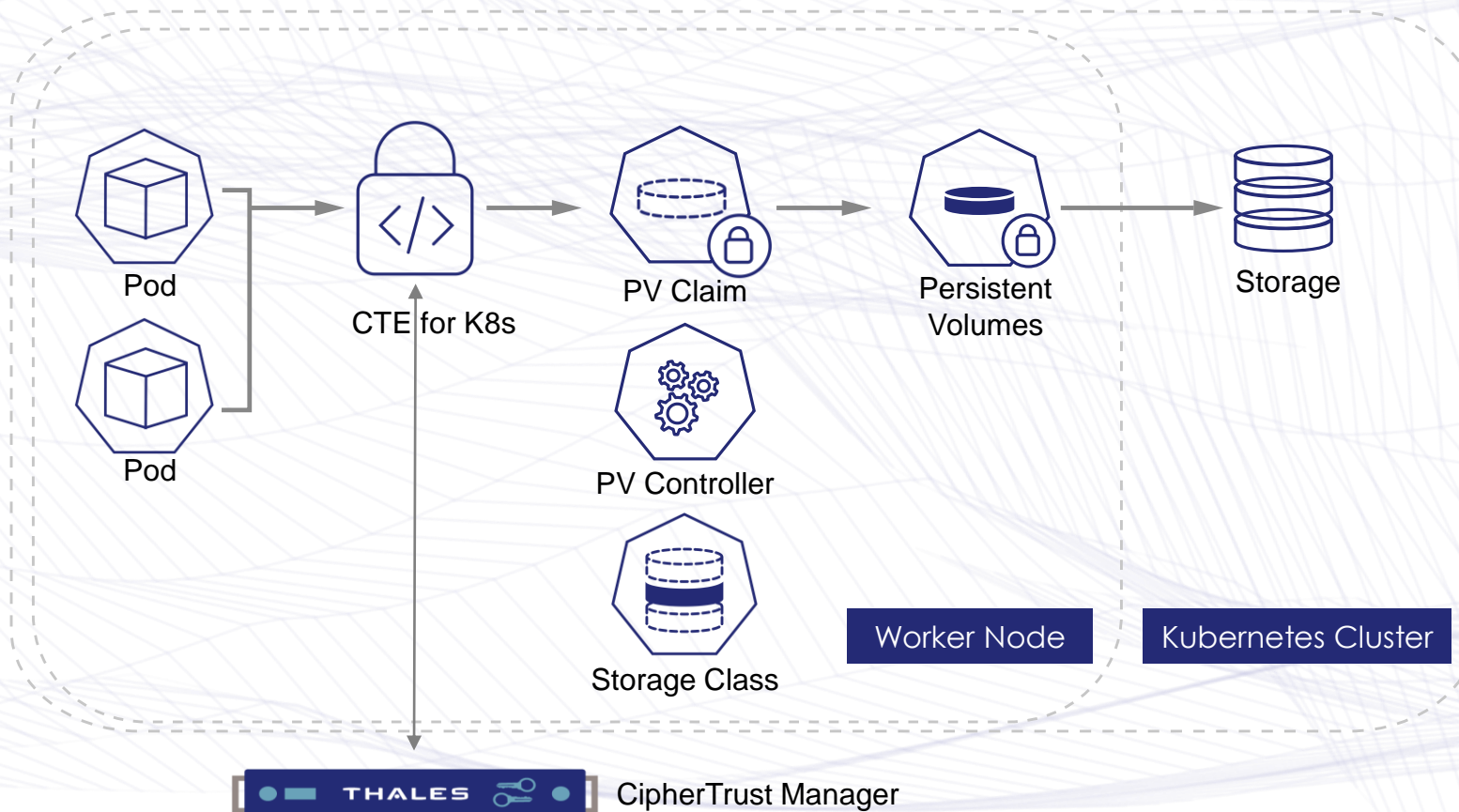
# CTE for K8s

도커 컨테이너 이미지 형태로 제공

Kubernetes 툴과의 연동을 통해 컨테이너 환경에서 투명한 파일 암호화 제공

내부적으로 Container Storage Interface 를 통해 동작

CM CE 와의 연동을 통해 3개의 Kubernetes Cluster 라이선스 제공



고맙습니다