THALES
Building a future we can all trust

PASCON 2021
2021 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

# 미래의 보안 과제와 향후 방향

2011. 11 .11

탈레스코리아 구병춘 이사

# 목차

## Thales Cloud Security Study

- 탈레스 클라우드 보안 연구

## Importance of Key Management

- 키 관리의 중요성

## Depending against Ransomware Attack

- 랜섬웨어 공격에 대응한 데이터 보안

THALES
Building a future we can all trust

# 2021 Thales Cloud Security Study

## 2021 탈레스 클라우드 보안 연구

www.thalesgroup.com

OPEN

# 연구 개요

THALES
Building a future we can all trust

COVID-19 대유행은 멀티클라우드 및 하이브리드 배포를 포함하여 클라우드 환경의 장기적 광범위한 채택을 가속화하고 있음.

2021년 탈레스 클라우드 보안 연구는 전 세계 2,600명 이상의 보안 전문가 및 경영진을 대상으로 광범위한 설문 조사 수행하여 특히, APAC 지역 750명 이상의 응답을 분석하여 클라우드 보안 동향을 결과 제시함.

# 멀티클라우드 채택이 광범위하여 복잡성이 가중됨

**58%**

of APAC organizations are using 2+ IaaS providers

**46%**

agree that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premises

**54**

Approximate weighted average of SaaS applications used by APAC organizations

**65%**

consider securing the combination of on-premises and cloud either ‘challenging’ or ‘very challenging’

# 보안 팀을 위한 클라우드 보안 정책 정의

**78%**

of APAC organizations involve security teams in cloud security decisions

**36%**

of APAC organizations' cloud security is run independently by security teams

**42%**

of APAC organizations' cloud security is run collaboratively by security and cloud delivery teams

# 갈 길이 먼 MFA 도입

ONLY

14%

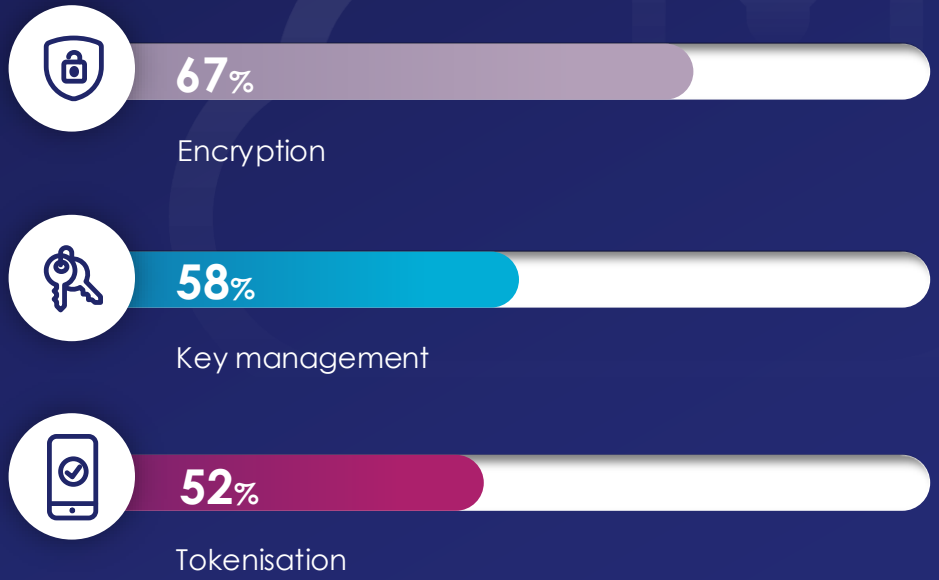
use MFA to secure more than half of their cloud services

ONLY

11%

use MFA to secure more than half of their on-premises applications

# 클라우드의 민감한 데이터를 보호하는 핵심 기술



# 클라우드 환경 보호를 위한 선도 기술

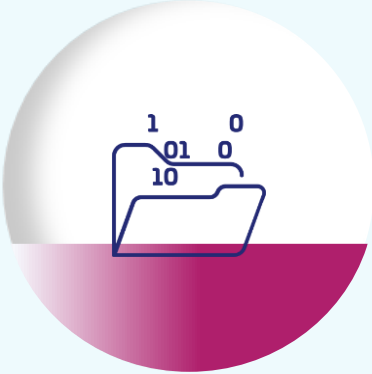
**39%**

Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Cloud Infrastructure Entitlement Management (CIEM)

**38%**

Encryption

**33%**




Data Loss Prevention (DLP)

**32%**

Multi-Factor Authentication (MFA)

# 시급한 클라우드 환경 암호화

**83%**

are encrypting less than half of sensitive data in the cloud

**25%**

have more than 50% of workloads in public clouds

**20%**

of respondents stated more than 50% of data in the cloud is sensitive

**61%**

rely on cloud providers to control all or most encryption keys when data is encrypted in the cloud

# 클라우드 환경에서 일반적인 데이터 유출 및 보안 감사 이슈

37%

have experienced a breach in their cloud environments

37%

have had either a breach or an audit issue on their cloud environments in the past 12 months

# 제로 트러스트 세상을 위한 최신 데이터 보안 전략

민감 데이터 검출

민감 데이터 암호화

암호 키 보호

사용자 접근 통제

THALES
Building a future we can all trust

# Importance of Key management

## 키 관리의 중요성

# 안전한 암호 키 관리 – SP 800-57

## 암호 키 생명 주기 관리

- 미 NIST에서 발간한 키 관리 표준

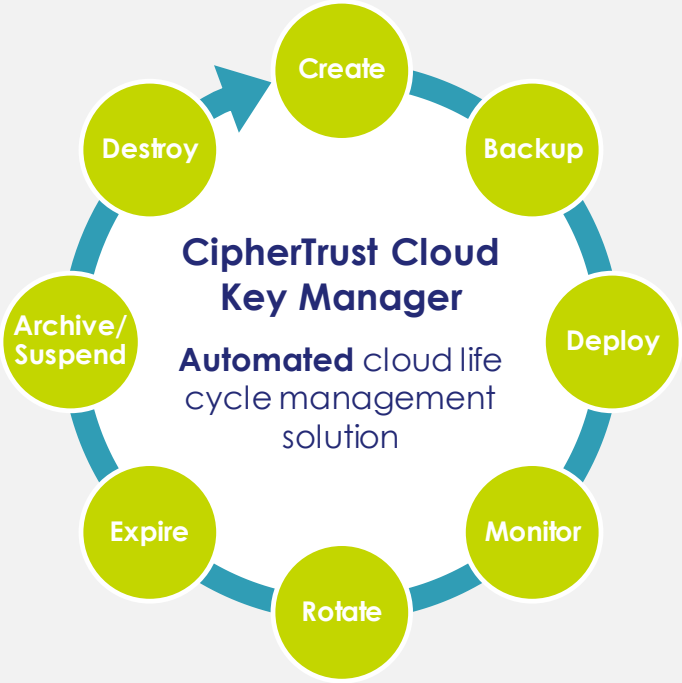
## 키 관리 솔루션

- 안전한 키 관리 필요성 증가
- HSM, KMS 등 전용 솔루션 도입 증가

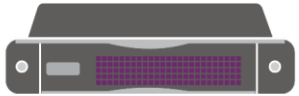
## 클라우드 키 관리

- 증가하는 클라우드 환경의 키 관리
- CSP 의 서비스 외 BYOK, HYOK 증가

**Key Life Cycle Management**



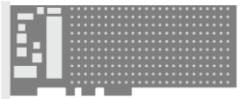
# HSM: Thales Luna 제품군



## SafeNet Luna Network HSM

- **고 가용성 및 확장 성**

- 일반적인 use cases:
  - Sub-CA key 저장
  - SSL/TLS offload
  - Database encryption
  - Code/Doc signing
  - Shared HSM access



## SafeNet Luna PCIe HSM

- **고성능 암호화 프로세서**

- 일반적인 use cases:
  - 번들 솔루션
  - 전용 HSM 성능이 필요한 애플리케이션서버에 설치

## SafeNet Luna USB HSM

- **오프라인 키 보관 및 HSM의 엔트리 모델**

- 일반적인 use cases:
  - Root CA's
  - Proof of concepts

# KMS: CipherTrust Manager

키 관리

접근 정책 관리

감사 보고서

유연한 API


FIPS 140-2 Compliant

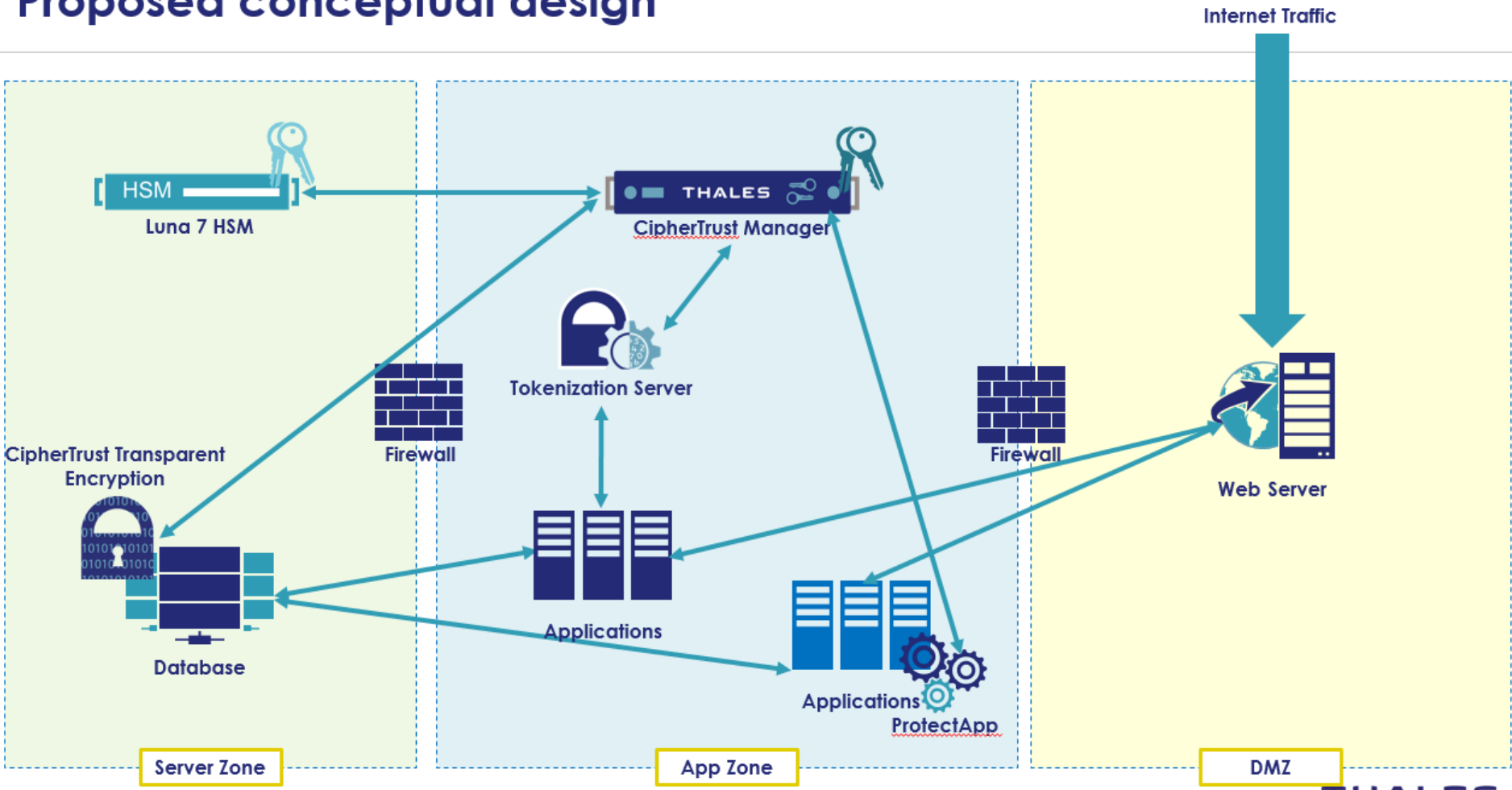

CipherTrust Manager

- 중앙 집중화된 키 관리 및 역할 기반 정책에 따른 통제
- 자사의 다양한 암호화 제품의 통합 관리 기능
- 다양한 로그 포맷 지원을 통해 향상된 감사 및 보고서 기능, 맞춤형 경보 기능
- 자동화된 암호화 및 관리 기능 구현을 위해 다양하고 유연한 REST API 지원
- 강력한 역할 분리(separation of duties) 와 Multi-tenant 지원
- 물리적 어플라이언스 또는 가상머신 형태로 제공 HSM 내장 또는 연동을 통해 FIPS 140-2 L 3 지원

# HSM 과 KMS 차이

| | HSM<br>(Hardware Security Module) | KMS<br>(Key Management System) |
|---|---|---|
| 도입 효과 | 보안의 중추 역할, KMS의 RoT 역할<br>소수의 키 관리 (Key Encryption Key) | 중앙 집중적 키 관리<br>다수의 키 관리 (Data Encryption Key) |
| 사용 편의성 | 낮음<br>대부분의 기능을 명령어 또는 API로 처리 | 높음<br>대부분의 기능을 GUI로 처리 |
| 보안성 | 높음<br>키는 항상 장비 내부만 존재함<br>True RNG 탑재 | 낮음<br>키를 필요로 하는 어플리케이션에 전달<br>Pseudo RNG 탑재 |
| 구성 기반 | 전용 하드웨어 | 범용 하드웨어 기반<br>최근 가상 머신 형태로 제공 |

# Proposed conceptual design



# CipherTrust Cloud Key Manager – 간결한 클라우드 키 관리

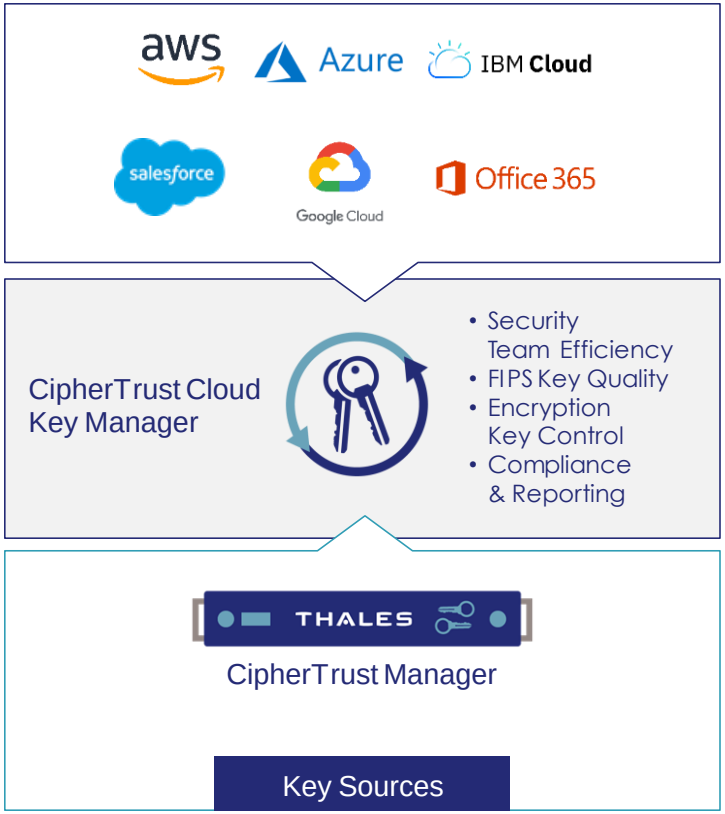
- FIPS 요구 수준을 충족하는 키 안정성 및 백업 지원
- 중앙 집중형, 높은 확정성, 편의성 제공
- 멀티 클라우드 및 하이브리드 클라우드 지원
- 암호 키 관리의 가시성 및 보고서 제공

## CCKM Appliance (v1.x) Integrations

- Microsoft Azure
- Microsoft Azure Stack
- Microsoft China and Germany National Clouds
- Amazon Web Services
- IBM Cloud
- Google Cloud CMEK* (Q3'20)
- Microsoft Office365
- Salesforce.com
- Salesforce Sandbox

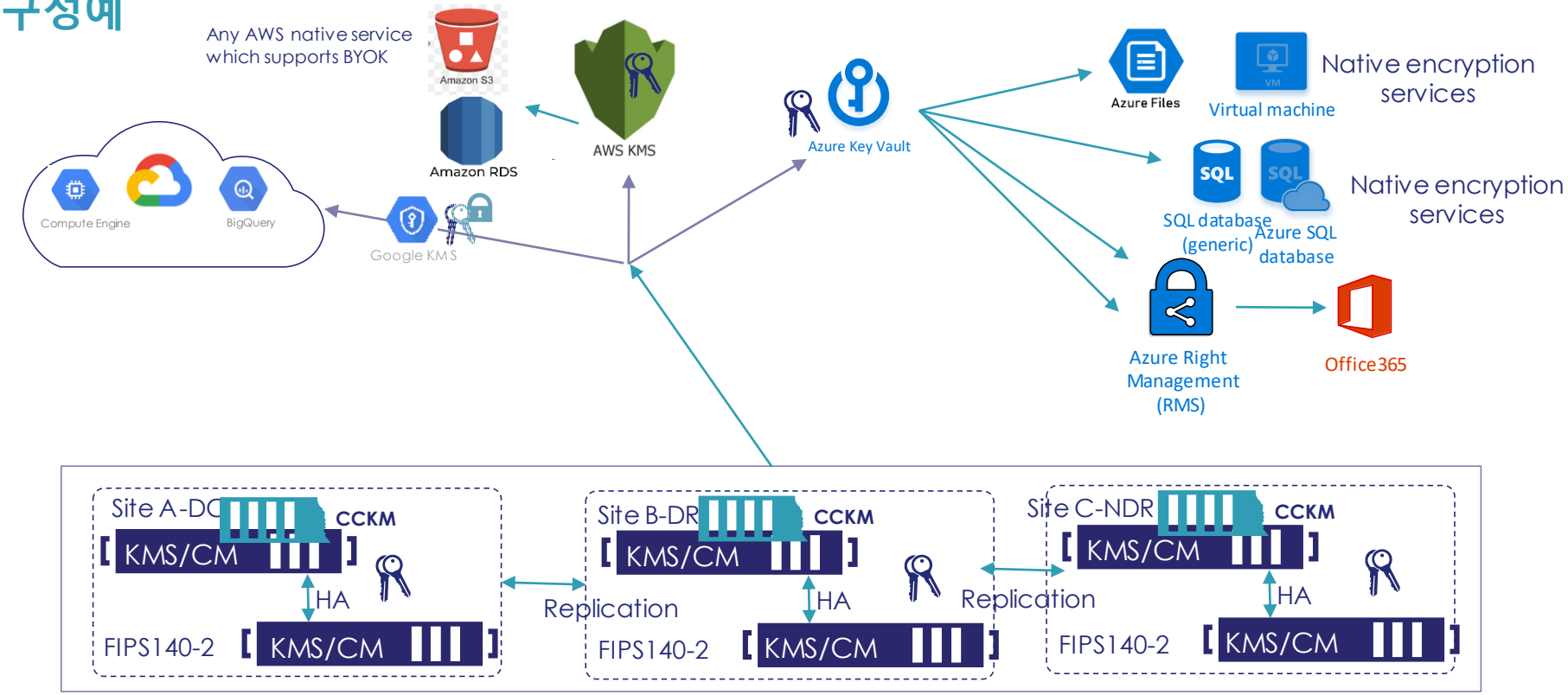
## CCKM Appliance (v2.x) Integrations

- Amazon Web Services: Amazon Gov Cloud and Amazon China Cloud
- Microsoft Azure: China and Germany National Clouds, Government Cloud and Azure Stack
- Microsoft Office365



# CCKM – CipherTrust Cloud Key Manager

## 구성예



THALES
Building a future we can all trust

# Depending against Ransomware Attack

## 랜섬웨어 공격에 대응한 데이터 보안

www.thalesgroup.com

OPEN

# 랜섬웨어 공격의 증가: 우리가 알아야 할 것들

## 출현빈도가 늘어남

**11 seconds**

올 해 11초마다 랜섬웨어 공격 발생

## 비용 증가

**4.44 million**

랜섬웨어 공격에 대한 비용

## 클라우드 적용 가속화

**Digital Transformation**

재택근무로 인한 클라우드 환경 적용

## 새로운 랜섬웨어 트랜드

- 이중 지불
- Ransomware-as-a-Service

1 – CyberSecurity Ventures – Global Ransomware Damage Costs
2 - 2020 IBM Cost of a Data Breach report
3. Twilio survey 92% of enterprises reported increased cloud migration

# 미디어에 나타난 최근 랜섬웨어 피해 사례



**백화점**

2020년 11월. 백화점및 그룹 리테일 망이 마비되고, 지역 영업망에 타격


**에너지 인프라**

2021년 5월. 5500 마일 의 파이프가 셧다운되고, 연료부족과 가격상승으로 이어짐


**의료분야**

2021년 9월. 독일 병원서버 마비로 병원진료 이상. 인명사고 발생

# 랜섬웨어 공격에 방어하기 위한 필수 요소

## 어플리케이션 화이트리스팅

- "신뢰할 수 있는 애플리케이션" 식별 – 중요 파일의 암호화/복호화를 수행하도록 승인된 바이너리
- 다형성 맬웨어가 승인된 바이너리에 들어가는 것을 방지하기 위해 서명을 사용하여 "신뢰할 수 있는 응용 프로그램"의 무결성을 확인하는 방법을 제공

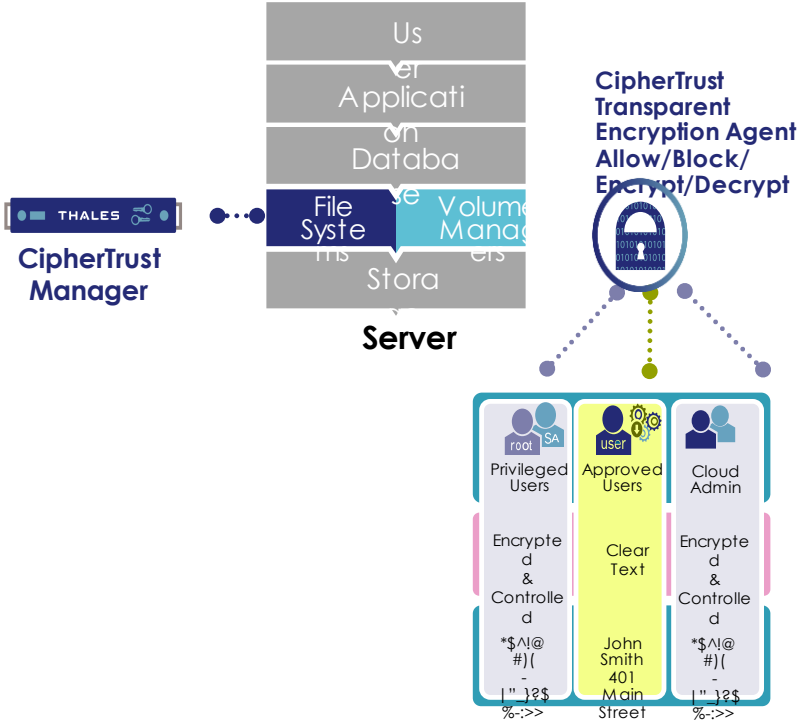
## 세분화된 접근 제어

- 누가(사용자/그룹) 특정 보호된 파일/폴더에 액세스할 수 있고 어떤 작업(암호화/복호화/읽기/쓰기/디렉토리 목록/실행)을 수행할 수 있는지 정의
- 특권 사용자(privileged user)라도 중요한 리소스를 검사하고 액세스하는 것을 방지

## Data-at-rest 암호화

- 온프레미스 데이터 센터 또는 퍼블릭/프라이빗 클라우드에 있는 데이터를 암호화
- 침입자가 비즈니스 크리티컬하거나 민감한 데이터를 훔치고 몸값을 지불하지 않으면 공개하겠다고 위협할 때 데이터를 무가치하게 만듭니다.

# CipherTrust Transparent Encryption




## 투명한 파일레벨 암호화

- 어느 정형, 비정형 데이터나 암호화

## Privileged user 의 접근 제어

- 루트권한의 사용자라고 하더라도, 사용자의 데이터에 접근하지 못함

## 데이터 접근 감사

- 위협 탐지를 가속화하고 포렌식을 용이하게 함

# CipherTrust Transparent Encryption 의 차별화된 기능

데이터 암호화에서 신뢰할 수 없는 바이너리 차단

CTE로 보호되는 시스템의 민감한 데이터에 액세스하는 "신뢰할 수 있는" 실행 파일에 대한 액세스 제어

민감한 데이터에 대한 액세스 제한

CTE로 보호되는 시스템의 중요한 데이터에 대한 관리자 집합의 제한없는 액세스 방지

민감한 데이터에 대한 모든 액세스 모니터링

CTE의 데이터 액세스 감사 로깅을 사용하여 데이터 개인 정보 보호 및 규정 준수 요구 사항을 충족

악성 맬웨어가 CTE로 보호되는 민감한 데이터를 암호화하는 것을 방지합니다

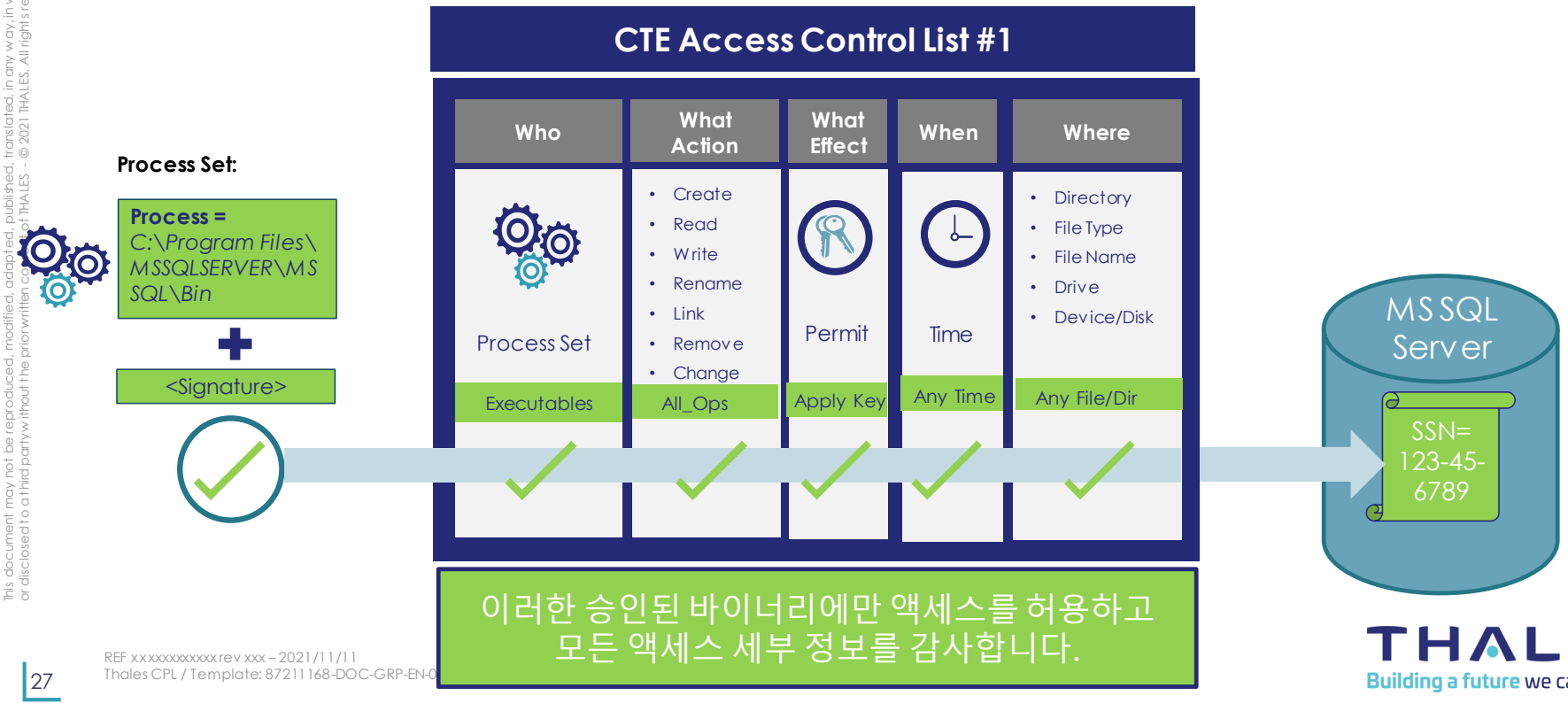
맬웨어가 권한 상승을 사용하여 민감한 데이터를 탈취하는 것을 방지합니다

맬웨어가 탐지를 방지하기 위해 트랙을 은밀하게 지우는 것을 방지합니다.

# CTE ACL 1: DB 파일 암호화 허용 하는 "응용 프로그램 화이트리스트" 정의

**파일/폴더를 암호화할 수 있는 애플리케이션(신뢰할 수 있는 바이너리) 정의 :**

- **Process Set:** *SQL-Processes= File/Folder: c:\Program Files\MSSQLSERVER\MSSQL\Bin\; <signature>*
- **ACL 1:** *Process= SQL-Processes; Action= All_Ops; Effect= Apply Key, Permit;*








THALES
Building a future we can all trust

# CTE ACL 2: 제한된 액세스

## 특권 사용자에 대한 제한된 액세스 권한 정의 :

- **User Set**: *Privileged-Admin-Users= Administrators, Domain Admins*
- **ACL 2**: *User= Privileged-Admin-Users; Action=read; Effect=Audit, Permit;*

참고: 특권 관리자(Previleged-Admin)도 키를 적용(암호화/복호화)하고 보호된 파일에 쓸 수 없습니다.

**User Set:**

**Privileged-Admin-Users:** *Administrators, Domain Admins*

### CTE Access Control List #2

| Who | What Action | What Effect | When | Where |
|---|---|---|---|---|
| User / Group<br>User Set | • Create<br>• Read<br>• Write<br>• Rename<br>• Link<br>• Remove<br>• Change | Permit | Time | • Directory<br>• File Type<br>• File Name<br>• Drive<br>• Device/Disk |
| Privileged Users | Read | Audit | Any Time | Any File/Dir |

MS SQL Server

1@X-Y3L!6W Q*+XZ

데이터를 복호화하지 않고 읽기 액세스를 허용하고 모든 액세스 세부 정보를 감사합니다.





THALES
Building a future we can all trust

# CTE ACL 3: DB 파일 암호화에서 다른 모든 바이너리 거부

## Define Default Deny Rule:

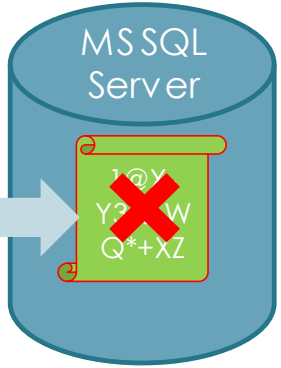
- **ACL 3**: *Default Deny Rule= Effect=Audit, Deny;*

**User Set:**

**NULL = DB 파일 접근이 허용되지 않은 나머지 사용자**

**CTE Access Control List #3**

| Who | What Action | What Effect | When | Where |
|---|---|---|---|---|
| User / Group<br>User Set | • Create<br>• Read<br>• Write<br>• Rename<br>• Link<br>• Remove<br>• Change | DENY | Time | • Directory<br>• File Type<br>• File Name<br>• Drive<br>• Device/Disk |
| All Users | All_Ops | Audit | Any Time | Any File/Dir |




보호된 모든 DB 파일에 대한 액세스를 거부하고 모든 액세스 시도를 감사합니다.





THALES
Building a future we can all trust

THALES
Building a future we can all trust

# 감사합니다.

Thales CPL

www.thalesgroup.com

OPEN