

# 아마존 웹서비스를 위한 탈레스 솔루션



## 아마존 웹서비스를 포함한 하이브리드 워크로드 보안

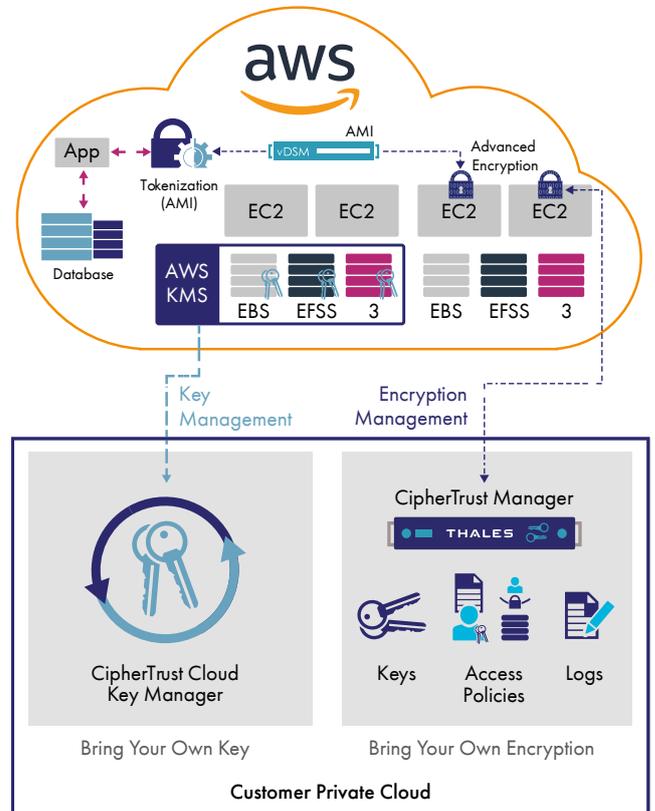
아마존 웹서비스는 IT 서비스를 편리하게 실행하고 비용을 절감할 수 있도록 지원합니다. 그러나 여전히 데이터 보호를 위한 최적의 운영절차는 필요하며, 다양한 보안, 프라이버시 및 규제 요구사항을 준수해야 합니다. 게다가 현재 사용 중인 모든 클라우드를 마이그레이션 할 경우를 대비한 신속한 데이터 이동성도 확보되어야 합니다. 만일, 특정 클라우드 벤더의 암호화 솔루션을 사용하게 된다면 이 기능이 약화될 수도 있습니다.

## 포괄적인 키 관리 기능을 탑재하고 있는 진보한 암호화 솔루션

효과적이고 안전하게 클라우드를 사용한다는 것은 사용자들이 데이터 보안에 대해 중요한 순간을 많이 마주하게 됨을 의미합니다. 즉, 클라우드에서 민감한 데이터를 다루는 일이 잦아짐을 의미합니다. 탈레스는 귀하의 디지털 트랜스포메이션을 안전하게 지켜드릴 수 있습니다. 탈레스의 고급 암호화 및 중앙집중식 키 관리솔루션은 온프레미스, AWS 및 다른 클라우드 제공업체에 저장된 데이터를 보호하고 제어할 수 있도록 지원합니다. 탈레스의 솔루션이 제공하는 기능은 다음과 같습니다.

- 암호화에 따른 종속성이 생기지 않습니다. 또한, 중앙 집중식 독립 암호화 운영기능을 통해 AWS를 포함한 다양한 클라우드 환경에 위치한 데이터 및 워크로드를 효과적이면서도 안전하게 분산시킬 수 있어 데이터 이동성이 확보됩니다.
- AWS KMS(Amazon Key Management Services: 아마존 키 관리 서비스)의 이점을 중앙 집중화된 키 관리 솔루션을 통해 멀티 클라우드로 확장하실 수 있습니다.

- 업계 선두의 SIEM 애플리케이션과 연계하여 데이터 접근 로깅을 활용함으로써 보다 빠르게 공격을 감지합니다.
- 볼트리스 토큰화 솔루션과 연동하면 보안 기능을 갖춘 애플리케이션 설계가 가능합니다



## Amazon 웹서비스 및 기타 클라우드를 위한 고급 암호화

IT 인프라가 100% AWS 기반인데 엄격한 내부 또는 업계의 데이터 보안 규제를 준수해야 할 경우, 또는 하이브리드 클라우드 기반이고 데이터가 기업 내 프라이빗 클라우드, AWS, 그리고 다른 클라우드 공급업체에 걸쳐 분산되어 있는 경우라면 고급 암호화 솔루션이 필요합니다. CipherTrust Transparent Encryption은 AWS를 비롯 여러 곳에 저장되어 있는 파일과 데이터베이스를 보호해 줍니다. 애플리케이션, 데이터베이스, 인프라 또는 비즈니스 절차, 그 어느 것도 바꿀 필요는 없습니다.

CipherTrust Transparent Encryption:

- 사용자(루트 권한을 가진 관리자 포함), 프로세스, 파일유형, 시간 등을 포함하는 세부적인 최소 권한 사용자 액세스 정책을 기반으로 무단 액세스를 통제 함으로써 데이터보안 강화
- 세부적인 파일 액세스 로그를 통해 규제 준수 요건 충족 및 침해 탐지 가속화 및 다양한 SIEM 솔루션과 연동 가능
- 운영에 지장을 주지 않는 유연한 구현 및 신속한 투자 회수. 암호화 에이전트는 AWS EC2 인스턴스 또는 스토리지에 액세스하는 기타 서버에서 실행되며 다양한 윈도우 및 리눅스 버전에서 사용 가능

## 중앙집중식 보안 키 관리

CipherTrust Manager는 AWS 용 CipherTrust Transparent Encryption에 대한 중앙화된 키, 정책 및 로그 관리를 제공합니다. DSM은 FIPS140-2 레벨2 또는 3에 부합하는 물리적 어플라이언스나 FIPS140-2 레벨1에 부합하는 가상 어플라이언스로 제공됩니다. 물리적 어플라이언스는 온프레미스 위치에서 전 세계 모든 클라우드 공급업체에 걸쳐있는 암호화 에이전트를 관리하는데 적합합니다. 가상 어플라이언스는 VMware, KVM, 아마존 웹서비스 AMI 및 마이크로소프트 애저 마켓플레이스에서 제공됩니다.

## PCI-DSS 규제 준수

Vormetric Tokenization with Dynamic Data Masking은 데이터 센터, 빅데이터 또는 클라우드 환경의 데이터를 간소화하고 익명화 시킴으로써 PCI-DSS 규제를 준수할 수 있도록 지원합니다. 형태 보존 및 랜덤 토큰화기능은 데이터베이스 구조를 유지하면서도 데이터의 민감한 필드를 보호할 수 있도록 지원합니다. 또한, 무중단 구현이 실현됩니다. 정책 기반 동적 데이터마스킹 기능의 경우 애플리케이션에 간단히 추가할 수도 있습니다. CipherTrust Tokenization Server는 공유형 AWS AMI로 사용할 수도 있습니다.

## AWS 암호키 관리

자체 암호화를 쓸수 없는 기업의 경우 CipherTrust Cloud Key Manager를 사용하여 외부에서 키를 관리함으로써 업계의 모범사례를 따를 수 있습니다.

CipherTrust Cloud Key Manager는 클라우드 서비스 업체의 키 관리 API를 활용하여 사용자가 중앙에서 가시성을 확보하고 중앙 집중식으로 관리할 수 있도록 지원합니다. 또한, 암호키의 라이프사이클을 중앙에서 관리함으로써 키관리의 복잡성과 운영비용을 줄일 수 있습니다. 본 솔루션은 서비스 형태로(As-a-Service) 제공되어 CipherTrust Key Manager를 통해 즉시 배포될 수도, 엄격한 규제 준수 사항을 지키기 위해 온프레미스 형태로 구축할 수도 있습니다.

CipherTrust Cloud Key Manager는 다음과 같은 이점을 제공합니다.

- 클라우드가 제공하는 규모, 비용 및 편의성의 혜택이 결합된 보다 안전한 키 관리
- 암호키에 대한 보다 강력한 제어-AWS KMS, 마이크로소프트 애저 등에서 사용되는 키 생성
- 키교체 및 포괄적인 암호키 수명주기 관리기능을 단일 콘솔을 통해 제공함으로써 멀티클라우드 암호키를 효과적으로 관리하며 IT 효율성 향상

## 데이터 보호 요구 사항 충족

탈레스는 Amazon Web Service 워크로드 보안을 간소화하고, 데이터 보안 규제를 준수할 수 있도록 지원합니다. CipherTrust Data Security Platform 제품은 AWS 워크로드에서 매끄럽게 운영됩니다. 또한, 탈레스 클라우드 키관리 솔루션은 사용자가 업계의 모범사례를 따르면서 데이터 보안 규제를 준수할 수 있도록 지원합니다

## 탈레스에 대하여

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한, 결정적인 기술.