

# CipherTrust Data Security Platform

## 검출, 보호, 관리

### CipherTrust Data Security Platform

차세대 통합 데이터 보안 플랫폼으로 데이터의 위치에 상관없이 민감데이터 검출, 보호 및 관리

검출

보호

통제

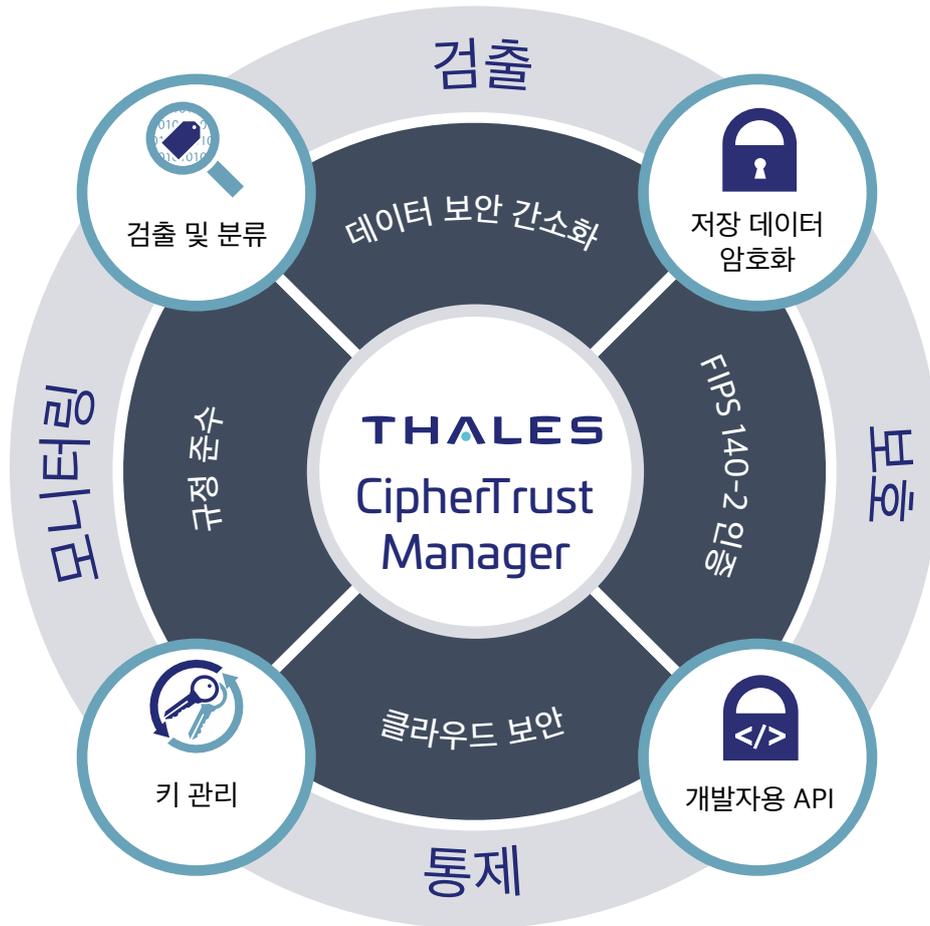


데이터 유출 사고가 계속 증가함에 따라 민감 데이터 보호는 모든 기업의 우선순위가 되었습니다. 또한 기업은 점점 진화하는 글로벌 및 자국의 개인정보 보호 규정을 준수함과 동시에, 원격 근무 증가에 수반되는 클라우드 위협에도 대처해야 합니다. IT 보안 팀은 네트워크에서 애플리케이션과 클라우드로 전송되는 데이터를 보호하기 위한 데이터 중심 솔루션을 모색하고 있습니다. 경계 네트워크 통제 및 엔드포인트 보안 체제가 무너지면 저장 데이터 보호 체제만이 최후의 방어선이 됩니다.

CipherTrust Data Security Platform은 데이터 검출, 분류, 보호 및 극도로 세분화된 접근 통제 절차를 중앙 집중식 키 관리 프로세스와 통합 지원합니다. 이 솔루션은 데이터 보안의 복잡성을 해소하고, 규정을 준수하는 데 소요되는 시간을 절약하며, 클라우드 마이그레이션 프로세스를 보호하는 데 이상적입니다. 따라서 데이터 보안 작업에 투입되는 인력을 줄이고, 포괄적 규정 준수 체계 구축이 가능하며, 비즈니스 전반에 걸친 위험 역시 크게 감소시킬 수 있습니다.

#### 주요 특징

- 중앙 집중식 관리 콘솔
- 모니터링 및 보고
- 데이터 검출 및 분류
  - 데이터 시각화를 통한 위험 분석
- 데이터 보호 기술
  - 파일, 데이터베이스 및 컨테이너 트랜스퍼런트 암호화
  - 애플리케이션 계층 데이터 보호
  - 형태 보존 암호화(FPE)
  - 동적 데이터 마스킹을 통한 토큰화
  - 정적 데이터 마스킹
  - 사용자 접근 권한 통제
- 중앙 집중식 엔터프라이즈 키 관리
  - FIPS 140-2 준수
  - 독보적인 KMIP 통합 파트너 에코시스템
  - 멀티 클라우드 키 관리
  - 데이터베이스 암호키 관리(Oracle TDE, 빅데이터, MS SQL, SQL Server Always Encrypted 등)



## 규정 준수

CipherTrust Data Security Platform은 다음과 같은 국제 보안 및 개인정보 보호 규정을 준수하는 데 유용합니다.

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- 남아프리카 POPI 법
- ISO/IEC 27002:2013
- 일본 마이넘버 규제
- 한국 개인정보보호법
- 인도 아다하르 법
- 필리핀 개인정보 보호법
- 싱가포르 모네테리 법
- 호주 개인정보 개정법

## 주요 효과

- **데이터 보안 간소화:** 차세대 통합 데이터 보호 솔루션을 통해 저장된 모든 기업의 민감 데이터를 검출, 보호, 통제할 수 있습니다. CipherTrust Data Security Platform은 민감 데이터를 검출하여 분류하고, 외부 위협에 대처하며, 내부자의 오용으로 발생하는 데이터 유출을 방지하고, 클라우드나 외부 서비스 제공업체의 인프라에 데이터가 저장되어 있는 경우에도 통제력을 발휘할 수 있는 강력한 기능을 보유한 단일 화면의 중앙 집중식 관리 콘솔을 통해 데이터 보안 관리를 간소화합니다. 기업은 디지털 혁신을 진행하기에 앞서 개인정보 보호 측면에서의 공백을 손쉽게 찾아내 해소하고, 데이터 보호를 최우선순위에 둠과 동시에 개인정보 보호 및 보안 지침에 관하여 신뢰할만한 정보에 근거한 결정을 내릴 수 있게 됩니다.
- **규정 준수를 위해 소요되는 시간 절약:** 기업은 민감 데이터를 적절히 통제하고, 이를 증명할 보고서를 규제 기관과 감사관에게 제출해야 합니다. 데이터 검출 및 분류, 암호화, 접근 통제, 감사 로그, 토큰화 및 키 관리 같은 CipherTrust Data Security Platform의 기능은 포괄적인 데이터 보안 및 개인정보 규정을 준수하는 데 매우 유용합니다. 이러한 기능을 통하여 새로운 환경에 추가되거나 빠르게 변화하고 진보하는 규정에 적극적으로 대응할 수 있습니다. 중앙 집중식과 확장성이란 플랫폼의 특성은 새로운 데이터 보호 요구 조건에 따라 라이선스를 추가로 구매하고 필요한 커넥터를 스크립트 기반으로 구축하여 새로운 통제 기능을 신속하게 추가할 수 있도록 도와줍니다.

- **안전한 클라우드 마이그레이션:** CipherTrust Data Security Platform은 기업이 민감 데이터를 클라우드에 안전하게 저장할 수 있도록 고급 암호화 및 중앙 집중식 키 관리 솔루션을 지원합니다. 이 플랫폼은 고급 멀티 클라우드 BYOE(Bring Your Own Encryption) 솔루션을 지원하므로 클라우드 서비스 제공업체의 암호화에 따른 종속성이 생기지 않으며, 독립적인 중앙 집중식 암호 키 관리를 통해 데이터를 다양한 클라우드에 효과적으로 분산시킬 수 있어 데이터의 이동성이 보장됩니다. BYOE 정책을 시행할 수 없는 기업은 CipherTrust Cloud Key Manager를 사용하여 외부에서 키를 관리하는 방법이 있으며, 타사의 모범 사례를 참고할 수 있습니다. CipherTrust Cloud Key Manager는 다양한 클라우드 인프라와 SaaS 애플리케이션에서 BYOK 용례를 지원합니다. CipherTrust Data Security Platform을 구현하면 가장 강력한 보호체계가 클라우드에 위치한 민감 데이터와 애플리케이션을 보호하므로 기업은 한결 수월하게 규정을 준수하고 모든 데이터가 생성, 사용 또는 저장되는 위치와 관계없이 보다 효과적인 통제가 가능합니다.

## CipherTrust Data Security Platform 제품

### CipherTrust Manager

CipherTrust Manager는 CipherTrust Data Security Platform의 중앙 관리를 위한 핵심 구성요소입니다. CipherTrust Manager는 기업이 암호키를 중앙에서 관리하고, 세분화된 접근 통제가 가능하며, 보안 정책을 구성할 수 있는 업계 최고의 엔터프라이즈 키 관리 솔루션입니다. CipherTrust Manager는 생성, 순환, 폐기, 가져오기, 내보내기를 포함한 주요 수명주기 작업을 관리하고, 역할 기반의 키 및 정책에 대한 액세스를 제어하며, 강력한 감사 및 보고 기능 지원과, 개발자 및 관리자 친화적인 REST API를 제공합니다. CipherTrust Manager는 FIPS 140-2 최대 Level 3 인증 수준의 물리적 및 가상 폼 팩터를 제공합니다. CipherTrust Manager는 Thales Luna 및 Luna Cloud HSM 같은 하드웨어 보안 모듈(HSM)과 통합이 가능합니다.

### CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification은 클라우드, 빅데이터 환경, 기존 데이터 저장소에 위치한 규제 대상 데이터(정형 및 비정형)를 검출합니다. 민감 데이터와 보안 위험도가 단일 관리자 화면에 일목요연하게 나열되므로 이를 바탕으로 보다 나은 결정을 통해 보안 공백을 메우고, 규정 위반 사례를 줄이며, 해결 우선순위를 정할 수 있습니다. 이 솔루션은 정책 구성, 검출 및 분류부터 위험 분석 및 보고에 이르기까지 최적화된 워크플로우를 통하여 보안의 사각지대와 복잡성을 해소하는 데 용이합니다.

### CipherTrust Transparent Encryption

CipherTrust Transparent Encryption은 저장 데이터 암호화, 사용자 접근 권한 통제, 상세한 데이터 접근 감사 로그 기능을 제공합니다. CipherTrust Transparent Encryption 에이전트는 클라우드와 빅데이터 환경에 구현된 실제 및 가상 서버의 Windows, AIX 및 Linux OS를 기반으로 하는 파일, 볼륨, 데이터베이스의 데이터를 보호합니다. CipherTrust Transparent Encryption에 사용할 수 있는 Live Data Transformation 확장 모듈은 무중단 데이터 암호화 및 재입력을 지원합니다. 또한 보안 분석 로그 및 보고서는 주요 보안 정보 및 이벤트 관리(SIEM) 시스템을 사용하여 규정 준수 보고 체계를 간소화하고 위험 탐지 속도를 가속화하는 데 도움이 됩니다.

### CipherTrust Application Data Protection

CipherTrust Application Data Protection은 API를 통해 키 관리, 서명, 해싱 및 암호화 서비스와 같은 기능을 지원하므로 개발자가 애플리케이션 서버 또는 빅데이터 노드의 데이터를 쉽게 보호할 수 있습니다. 이 솔루션은 샘플 코드를 제공하므로 개발자가 애플리케이션에서 처리된 데이터를 안전하게 보호할 수 있습니다. CipherTrust Application Data Protection은 개발자가 맞춤형 데이터 보안 솔루션을 개발하는 데 소요되는 시간을 줄이는 한편, 키 관리의 복잡성을 제거합니다. 또한 이 솔루션은 보안 운영팀이 전담으로 관리하는 키 관리 정책을 통해 강력한 역할 분리를 가능케 합니다.

### CipherTrust Tokenization

CipherTrust Tokenization은 볼티드(Vaulted) 방식 제품과 볼트리스(Vaultless) 방식 제품으로 출시되어 있으며, PCI-DSS 같은 데이터 보안 규정을 준수하는 데 수반되는 비용과 복잡성을 제거하는 데 유용합니다. CipherTrust Tokenization은 민감 데이터를 그에 상응하는 토큰으로 대체하므로 데이터베이스와 인증받지 않은 사용자 및 시스템으로부터 민감 데이터를 철저히 보호할 수 있습니다. 볼트리스 방식 제품은 정책 기반의 동적 데이터 마스킹 기능을 포함하고 있습니다. 두 가지 제품 모두 애플리케이션에 토큰화를 쉽게 추가할 수 있도록 설계되어 있습니다.

### CipherTrust Database Protection

CipherTrust Database Protection 솔루션은 데이터베이스의 민감 데이터 암호화 방식을 안전한 중앙 집중식 키 관리 체계와 통합하며, 데이터베이스 애플리케이션을 수정하지 않고도 사용 가능합니다. CipherTrust Database Protection 솔루션은 Oracle, Microsoft SQL Server, IBM DB2, Teradata 데이터베이스를 지원합니다.

### CipherTrust Key Management

CipherTrust Key Management는 전사적으로 암호키를 관리할 수 있는 강력한 표준 기반 솔루션을 제공합니다. 암호키 관리에 수반되는 문제를 완화하는 데 유용한 이 솔루션은 암호키를 보호하고 반드시 인증받은 암호화 서비스에만 키를 프로비저닝합니다. CipherTrust Key Management 솔루션은 다음과 같은 다양한 용례를 지원합니다.

- **CipherTrust Cloud Key Manager**는 Amazon Web Services, Microsoft Azure, Salesforce, IBM Cloud용 BYOK 관리를 간소화합니다. 이 솔루션은 포괄적인 클라우드 키 수명주기 관리 및 자동화를 통해 보안 팀의 업무 효율성을 향상시키며, 클라우드 키 관리를 간소화 시킵니다.
- **CipherTrust TDE Key Management**는 Oracle, Microsoft SQL, Microsoft Always Encrypted 같은 다양한 데이터베이스 솔루션을 지원합니다.
- **CipherTrust KMIP Server**는 전체 디스크 암호화(FDE), 빅데이터, IBM DB2, 테이프 아카이브, VMware vSphere 및 vSAN 암호화 등과 같은 KMIP 클라이언트를 중앙 집중식으로 관리하는 데 이상적입니다.

## 탈레스 소개

개인정보를 중요시하는 기업들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스의 보안 솔루션을 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.