cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform
검출, 보호, 통제

IT 팀은 네트워크에서 애플리케이션과 클라우드로 전송되는 데이터를 보호하기 위한 데이터 중심 솔루션을 물색하고 있습니다. 오늘날 경계 네트워크 통제 및 엔드포인트 보안 체제가 무너지는 가운데 기업이 진화하는 개인정보 보호 규정을 준수하는 동시에 급증하는 원격 근무 직원들을 지원하려면 데이터 중심 솔루션이 필요하기 때문입니다.

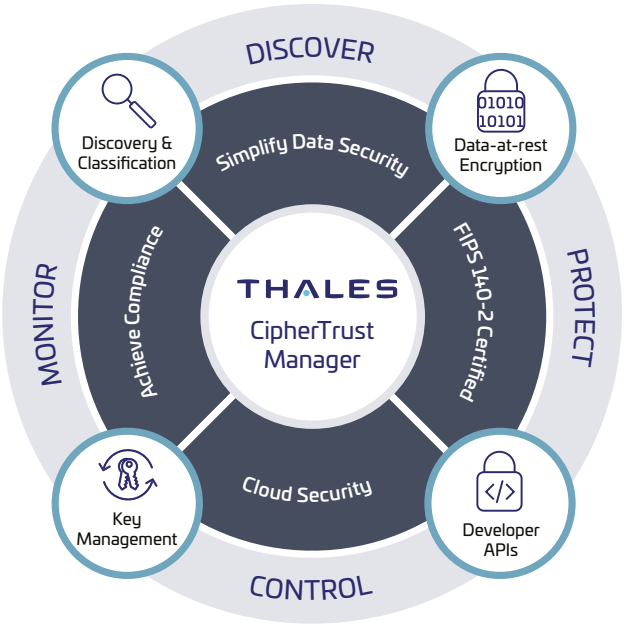
CipherTrust Data Security Platform(CDSP)은 기업의 위험을 크게 줄일 뿐만 아니라 강력한 데이터 보안을 유지하는 데 필요한 리소스까지 줄일 수 있는 데이터 중심 솔루션입니다.

CDSP는 데이터 검출, 분류, 보호 및 세분화된 접근 통제 절차를 중앙 집중식 키 관리 프로세스와 통합 지원합니다. 또한 데이터 보안을 중앙에서 관리하고 간소화하여 규정 준수 시간을 단축하고 클라우드 마이그레이션을 안전하게 보호합니다.

주요 특징

- 중앙 집중식 관리 콘솔
- 모니터링 및 보고
- 데이터 검출 및 분류
  - 데이터 시각화를 통한 위험 분석
- 데이터 검출 및 분류를 트랜스페어런트 암호화와 결합하여 파일 수준에서 민감 데이터를 자동으로 암호화
- 랜섬웨어 차단
  - 악의적인 동작을 능동적으로 감시
  - 동작 모니터링 및 데이터 분석 활성화:
    - 제로-데이 공격 차단
    - 시스템에서 인터넷 연결 중단 시 보호
    - 엔드포인트에서 랜섬웨어 탐지 후 설치 시 보호
- 시크릿 관리
  - 모든 유형의 시크릿을 중앙에서 관리
  - DevOps 통합, 자동화 및 오케스트레이션에서 사용 편의성을 고려한 설계
  - 하이브리드, 멀티-클라우드(모든 클라우드), 멀티-테넌트, 온프레미스, 레거시 시스템에서 사람 또는 시스템 접근에 사용되는 시크릿 관리

- 데이터 보호 기술
  - 파일, 데이터베이스 및 빅데이터 트랜스페어런트 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 암호화 키 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 준수합니다.

- 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 모네터리 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 온프레미스 및 클라우드 기반 데이터가 저장되어 있는 경우에도 통제력을 발휘할 수 있는 강력한 기능을 보유한 중앙 집중식 관리 콘솔을 통해 데이터 보안 관리를 간소화합니다. 기업은 운영 방식을 근본적으로 변경하여 고객 가치를 창출하는 디지털 혁신을 시작하거나 진행하기에 앞서 개인정보 보호 측면에서의 공백을 손쉽게 찾아내 해소하고, 랜섬웨어를 탐지하여 차단하며, 비밀 코드를 관리하고, 데이터 보호를 최우선 순위에 둠과 동시에 개인정보 보호 및 보안 지침에 관하여 신뢰할 만한 정보에 근거한 결정을 내릴 수 있습니다.
- **규정 준수를 위해 소요되는 시간 절약.** 기업은 민감 데이터를 적절히 통제하고, 이를 증명할 보고서를 규제 기관과 감사관에게 제출해야 합니다. CDSP는 데이터 검출 및 분류, 랜섬웨어 차단, 시크릿 관리, 암호화, 접근 통제, 감사 로그, 토큰화, 키 관리 등 포괄적인 데이터 보안 및 개인정보 보호 요건을 지원합니다. 이러한 데이터 보안 통제 기능을 점차 진화하는 규정 준수 요건에 대응하여 새로운 배포 환경에 추가할 수 있습니다. 이 플랫폼은 중앙 집중식 관리 및 확장성 덕분에 라이선스를 추가하고 스크립트 작성 방식으로 배포하여 새로운 통제 기능을 빠르게 추가할 수 있습니다.
- **안전한 클라우드 마이그레이션.** CipherTrust Data Security Platform은 기업이 민감 데이터를 클라우드에 안전하게 저장할 수 있도록 고급 암호화, 중앙 집중식 시크릿 관리, 중앙 집중식 키 관리 솔루션을 지원합니다. 이 플랫폼은 고급 멀티 클라우드 BYOE(Bring Your Own Encryption) 솔루션을 지원하므로 클라우드 서비스 제공업체에 따른 종속성이 생기지 않으며, 클라우드 중립적인 중앙 집중식 암호화 키 관리를 통해 데이터를 다양한 클라우드에 효과적으로 분산시킬할 수 있어 데이터의 이동성이 보장됩니다. BYOE 정책을 시행할 수 없는 기업은 CipherTrust Cloud Key Management(CCKM)를 사용하여 외부에서 키를 관리하는 방법으로 업계의 모범 사례를 따를 수 있습니다. CCKM은 BYOK(Bring Your Own Key) 및 HYOK(Hold Your Own Key) 사용 사례를 지원하고, 다양한 클라우드 인프라와 SaaS 애플리케이션에서 네이티브 키 관리를 간소화합니다. Akeyless Vault를 기반으로 하는 CipherTrust Secrets Management는 모든 유형의 시크릿을 자동으로 생성, 저장, 교체, 폐기할 수 있는 프로세스를 포함해 엔터프라이즈급 시크릿 수명 주기 관리를 제공합니다.

CipherTrust Data Security Platform

CDSP는 CipherTrust Manager(CM)와 커넥터 세트로 구성됩니다.

CM은 온프레미스, 클라우드 또는 하이브리드 환경에 배포하거나, 서비스 형태로 구독할 수 있습니다.

CipherTrust Manager

CDSP의 중앙 관리 지점인 CM은 모든 암호 키를 대상으로 키 수명 주기 관리 작업을 간소화합니다. 또한 보안 키 생성, 백업/복구, 클러스터링, 비활성화, 삭제, 다양한 사용 사례(예: 데이터 검출, 저장 데이터 암호화, 엔터프라이즈 키 관리, 클라우드 키 관리)를 지원하는 커넥터 및 파트너 통합에 대한 접근을 관리합니다. 그 밖에도 키 및 정책에 대한 역할 기반 접근 통제와 강력한 감사 및 보고를

지원하고, 개발자/관리자 친화적인 REST API를 제공합니다. CM은 물리적 폼 팩터와 가상 폼 팩터 모두에서 제공됩니다. 하드웨어 및 가상 어플라이언스는 임베디드 Luna Network HSM을 이용하거나 클라우드 HSM을 선택하여 가장 높은 신뢰 루트인 FIPS 140-2 Level 3를 활성화할 수 있습니다.

CipherTrust Data Discovery and Classification(DDC)

DDC는 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(CTE)

CTE는 저장 데이터 암호화, 사용자 접근 권한 통제, 상세한 데이터 접근 감사 로그 기능을 제공합니다. 에이전트는 클라우드와 빅데이터 환경에 구현된 물리/가상 서버의 Windows, AIX, Linux 운영 체제에서 파일, 볼륨 및 데이터베이스의 데이터를 보호합니다. CTE에 사용할 수 있는 Live Data Transformation 확장 모듈은 무중단 데이터 암호화 및 키 로테이션을 지원합니다. 또한 보안 분석 로그 및 보고서는 주요 보안 정보 및 이벤트 관리(SIEM) 시스템을 사용하여 규정 준수 보고 체계를 간소화하고 위협 탐지 속도를 높이는 데 도움이 됩니다.

CipherTrust Transparent Encryption Ransomware Protection(CTE- RWP)

CTE-RWP는 동작 모니터링을 통해 의심스러운 활동을 감시하면서 랜섬웨어 지표가 탐지되면 프로세스를 차단합니다. CTE- RWP는 멀웨어 서명 데이터베이스가 아닌 동작 모니터링과 데이터 분석을 사용하기 때문에 네트워크 연결이 끊어지더라도 제로-데이 공격에서 시스템을 보호합니다. 그 밖에도 배포 및 관리가 매우 쉽습니다.

Akeyless Vault 기반 CipherTrust Secrets Management(CSM)

CSM은 Akeyless Vault Platform을 기반으로 하는 최첨단 엔터프라이즈급 시크릿 관리 솔루션입니다. CSM은 DevOps 도구나 클라우드 워크로드에서 자격 증명, 인증서, API 키, 토큰 같은 시크릿에 대한 접근을 보호하고 자동화합니다. DevSecOps 팀은 시크릿 관리를 멀티 클라우드 애플리케이션에 빠르고 쉽게 통합하여 CI/CD 프로세스를 안전하게 보호하고 가속화할 수 있습니다. 그 밖에도 배포 및 관리가 매우 쉽습니다.

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection은 기업이 민감도, 취약점, 위험 프로파일을 기준으로 데이터를 빠르게 검출하고 분류한 후 암호화와 접근 통제를 통해 위험에 노출된 데이터를 선제적으로 보호할 수 있는 제품입니다. 이 제품은 DDC와 CTE를 통합하여 운영 효율을 개선하고, 규정 준수 시간을 단축하며, 보안 공백을 선제적으로 해결합니다.

CipherTrust Application Data Protection

CADP는 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. CADP는 맞춤형 데이터 보안 솔루션 개발 시간을 단축하는 한편, 키 관리의 복잡성을 제거합니다. 또한 보안 운영팀이 전담으로 관리하는 키 관리 정책을 통해 강력한 역할 분리를 지원합니다.

CipherTrust Tokenization

CipherTrust Tokenization은 볼티드(Vaulted) 방식 제품과 볼트리스(Vaultless) 방식 제품으로 출시되어 있으며, PCI-DSS 같은 데이터 보안 규정 준수에 수반되는 비용과 복잡성을 제거하는 데 유용합니다. Tokenization은 민감 데이터를 그에 상응하는 토큰으로 대체하므로 데이터베이스와 인증받지 않은 사용자 및 시스템으로부터 민감 데이터를 분리하여 안전하게 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

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

CipherTrust Key Management

CipherTrust Key Management는 전사적으로 암호화 키를 관리할 수 있는 강력한 표준 기반 솔루션을 제공합니다. 암호화 키 관리에 수반되는 문제를 간소화하는데 유용한 이 솔루션은 키를 안전하게 보호하고 항상 승인된 암호화 서비스에만 키를 프로비저닝합니다. CipherTrust Key Management 솔루션은 다음과 같이 다양한 사용 사례를 지원합니다.

- **CCKM(CipherTrust Cloud Key Management)은** Amazon Web Services(AWS), Google Cloud Platform(GCP), Microsoft Azure[1], Oracle Cloud Infrastructure(OCI)[1], Salesforce 및 SAP[1]에서 "BYOK(Bring Your Own Key)"와 "HYOK(Hold Your Own Key)" 및 네이티브 키 관리를 간소화합니다. CCKM은 모든 클라우드 키가 네이티브 키일 때조차 운영 부담을 줄이고 효율을 높입니다. 또한 수명 주기 제어, 클라우드 내외에서 중앙 집중식 관리, 클라우드 암호화 키에 대한 가시성을 제공하여 키 관리 복잡성을 줄이고 운영 비용을 절감합니다.
- **CipherTrust TDE Key Management는** Oracle, Microsoft SQL, Microsoft Always Encrypted 등 광범위한 데이터베이스 솔루션을 지원합니다.
- **CipherTrust KMIP Server는** 전체 디스크 암호화(FDE), 빅데이터, IBM DB2, 테이프 아카이브, VMware vSphere, vSAN 암호화 같은 KMIP 클라이언트에 대한 중앙 집중식 관리를 지원합니다.

1 이 클라우드에 대한 HYOK 지원 날짜는 별도로 문의하십시오.

연락처 – 서울특별시 용산구 독서당대로 98 6층 탈레스 코리아 82.2.3278.8202