cpl.thalesgroup.com

THALES
Building a future we can all trust

쿠버네티스용 CipherTrust Transparent Encryption

당면 과제: 쿠버네티스 환경용 애플리케이션 보호하기

구성과 종속성으로 패키징된 마이크로서비스인 컨테이너를 사용해 구축되는 애플리케이션이 점차 많아지고 있습니다.
쿠버네티스는 이러한 컨테이너를 배포 및 관리하는 오픈소스 소프트웨어입니다. 컨테이너화된 애플리케이션은 쿠버네티스를 통해 더 빠르게 전달, 배포 및 관리하여 향상된 편의성을 제공할 수 있으며, 이는 최적화된 자원 활용 및 라이선스 비용 절감을 통한 재사용 가능한 모듈 구성 요소와 비용 절감을 통해 실현됩니다.
그러나 여기에는 다음과 같은 위험이 있습니다.

- **권한 있는 사용자의 남용.** 도커 프로세스는 기본적으로 루트 권한으로 실행되며 관리자는 모든 사용자 기밀 정보(tenant secrets)에 자유롭게 액세스할 수 있습니다. 하지만 이러한 무제한 자유로운 액세스 수준은 여러 위험을 초래합니다. 관리자가 컨테이너 이미지와 컨테이너 안에 저장된 데이터에 대해 확인되지 않은 액세스 권한을 지닌 경우에는 조직이 권한 상승 공격의 대상이 될 수 있습니다.
- **교차 컨테이너 액세스.** 권한이 잘못 구성되면 비공개로 유지되어야 하는 정보에 다수의 컨테이너가 액세스 권한을 갖게 될 수 있습니다.
  또한 컨테이너가 공유 가상 환경이나 클라우드 환경에서 호스팅되는 경우면 중요한 정보가 외부에 노출될 수 있습니다.
- **규정 준수 위험.** 많은 규정 준수 권한 의무에는 엄격한 액세스 제어와 데이터 액세스 감사가 필요합니다.
  하지만 보안 팀들은 대체로 컨테이너와 이미지에 저장된 데이터에 대한 액세스를 관리하고 추적 할 수 있는 제어 기능이 한정적입니다.
  결과적으로 이러한 팀은 관련 보안 정책과 규제 의무를 준수하기가 어렵습니다.

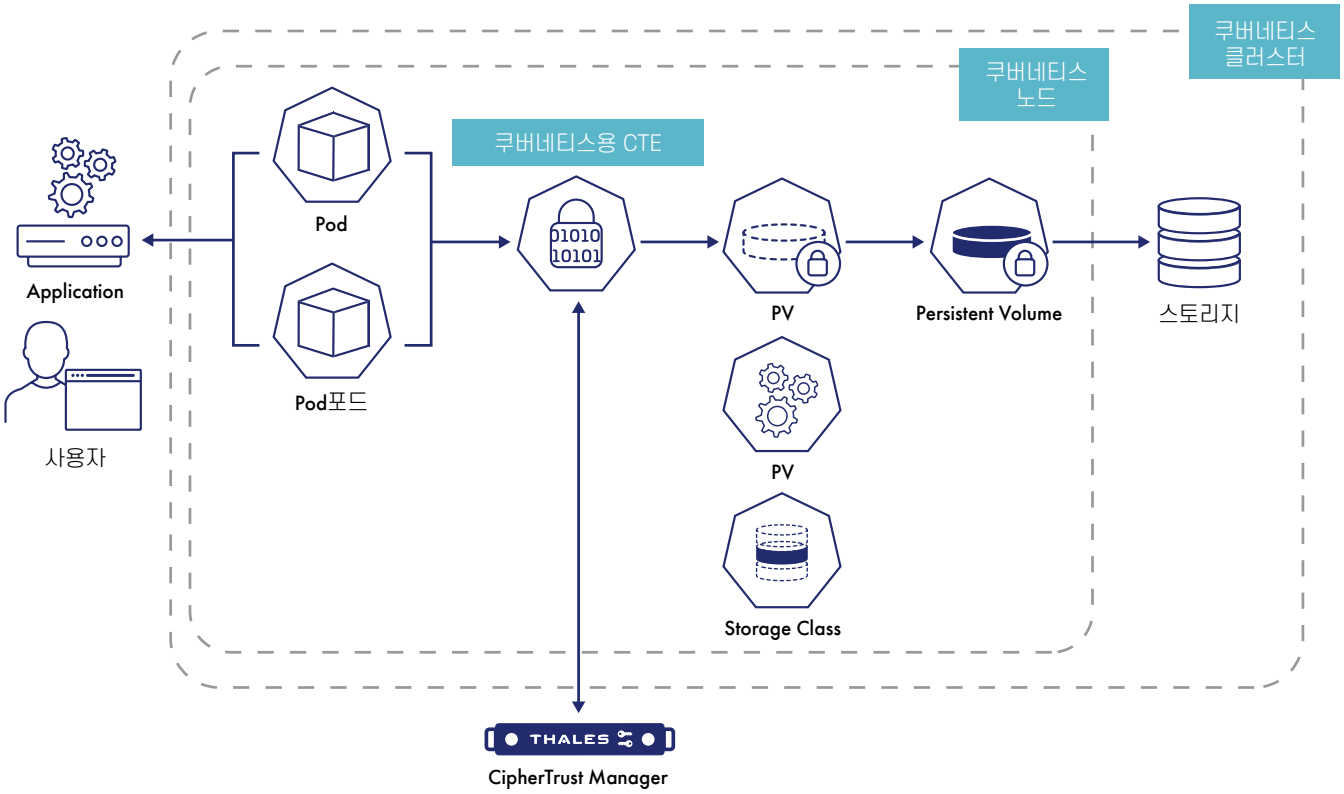
솔루션: 쿠버네티스를 위한 CipherTrust Transparent Encryption

쿠버네티스용 CipherTrust Transparent Encryption은 암호화, 액세스 제어 및 데이터 액세스 로깅을 위한 컨테이너 내 기능을 제공하여 조직이 쿠버네티스 환경에서 데이터를 중심으로 강력한 보호조치를 구축할 수 있게 해줍니다.
CipherTrust Transparent Encryption을 위한 이러한 확장을 통해 컨테이너 내부 데이터와 컨테이너에서 액세스할 수 있는 외부 스토리지의 데이터에 대한 데이터 보호를 컨테이너 단위로 적용할 수 있으며, 이를 CipherTrust Manager로 중앙에서 관리할 수 있습니다.

장점

쿠버네티스를 위한 CipherTrust Transparent Encryption은 다음과 같은 장점을 제공합니다.

- **규정 준수.** CipherTrust Transparent Encryption의 이러한 확장은 지불 카드, 의료 서비스 기록, 기타 중요 자산과 같은 중요한 데이터를 보호하기 위한 규정 준수 요구 사항 및 규제 의무를 해결합니다.
- **권한 있는 사용자에 대한 위협 차단.** 이 솔루션은 데이터 액세스 제어를 통한 암호화를 제공하므로 Docker나 OpenShift 클러스터 관리자와 같은 권한 있는 사용자가 중요한 데이터에 무단으로 액세스하지 않고도 일반 사용자 자격으로 작업할 수 있습니다.
- **강력한 보안 달성.** 쿠버네티스용 CipherTrust Transparent Encryption은 데이터 센터, 가상화 환경, 클라우드 구현 등 컨테이너가 저장되거나 사용되는 모든 곳에서 데이터 보안 정책을 시행합니다. 애플리케이션, 컨테이너 또는 인프라 세트를 변경할 필요 없이 비용 효율성, 제어 또는 성능을 보장하기 위해 컨테이너를 배포하고 사용합니다.



기능

- **포괄적인 데이터 보호 조치.** 쿠버네티스용 CipherTrust Transparent Encryption은 CipherTrust Transparent Encryption을 확장하여 보안 팀이 컨테이너 내부에 데이터 보안 제어 기능을 구축할 수 있게 해줍니다.
  이러한 확장을 통해 암호화, 액세스 제어, 데이터 액세스 로깅을 컨테이너 단위로 적용할 수 있습니다.
  컨테이너 내에 로컬로 생성 및 저장된 데이터, 그리고 컨테이너에서 네트워크 파일 시스템에 의해 마운트된 데이터에 암호화를 적용할 수 있습니다.
- **확장 가능한 투명한 암호화.** 애플리케이션, 컨테이너 또는 인프라 세트를 변경할 필요 없이 데이터 보안 제어기능을 제공합니다. 쿠버네티스 클러스터 내 모든 컨테이너에 단일 정책을 적용하거나, 클러스터 내 각 컨테이너에 별도의 정책을 적용할 수 있습니다.
  이 솔루션은 비즈니스 요구사항의 변화에 따라 쿠버네티스 환경을 확장하거나 축소할 수 있습니다.
- **세분화된 액세스 제어 및 가시성.** 쿠버네티스용 CipherTrust Transparent Encryption은 가장 엄격한 정책과 의무를 준수하는 데 필요한 상세한 가시성과 제어기능을 제공합니다.
  기업은 이 쿠버네티스 보안 솔루션을 통해 컨테이너 내 특정 사용자와 프로세스 및 리소스 세트를 기반으로 세분화된 액세스 정책을 수립할 수 있습니다.
  마지막으로, 이 솔루션은 컨테이너 간 격리를 설정할 수 있으므로 오직 권한이 있는 컨테이너만이 중요한 정보에 액세스할 수 있습니다.

CipherTrust Manager

CipherTrust Manager는 CipherTrust Transparent Encryption을 포함한 CipherTrust Data Security Platform을 위해 키, 정책 및 로그 관리를 중앙 집중화합니다.
높은 신뢰 루트로 마스터 키를 안전하게 저장하기 위해 가상 및 물리 폼팩터 모두에서 사용할 수 있습니다.
이러한 어플라이언스는 프라이빗 또는 퍼블릭 클라우드 인프라 뿐만 아니라 온프레미스에도 배포할 수 있습니다.

탈레스 클라우드 보호 솔루션 및 라이선스 정보

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안 측면에서 결정적인 순간에 직면하곤 합니다. 암호화 전략을 구축하거나, 클라우드로 이전, 규정 준수 의무를 충족해야 할 때 탈레스와 함께 디지털 혁신을 지속할 수 있습니다.

결단이 필요한 순간을 위한 결정적 솔루션

연락처 - 모든 사무실 위치 및 연락처 정보는 **cpl.thalesgroup.com/contact-us**를 참조하시기 바랍니다.