cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Platform Community Edition

몇 주가 소요되던 데이터 보호 추가 시간을 몇 분으로 단축

비즈니스 문제

데이터 보호 기능을 추가하는 데 소요되는 시간을 단축하면 보다 짧은 시간 안에 더 많은 작업을 수행할 수 있습니다.

기존의 데이터 보호 도구에서는 데이터 보호 기능을 삽입하려면 개발자가 코드를 수정해야 하는 등 애플리케이션 수정이 필요했습니다. 또한, 데이터 변경(새 필드, 삭제된 필드)이나 데이터 보호 방법의 변경(암호/키/매개변수 변경)이 발생할 때마다 개발자가 데이터 보호 코드를 수정해야 했습니다.

데이터나 데이터 보호 방법의 변경은 자주 발생하는 일입니다. 기존 데이터 보호 도구를 사용하는 개발자는 데이터 보호 코드를 수정하는 데 중점을 두고 반복적으로 작업을 중단하기 때문에 다른 프로젝트에서 제대로 속도를 내지 못했습니다.

CipherTrust 솔루션

Thales CipherTrust Platform Community Edition은 개발 프로세스에서 데이터 보호를 위한 새로운 작업의 추가 없이데이터 보호를 자동화하여 데이터와 파일을 보호하고 작업 속도를 유지할 수 있게 해줍니다. 또한, Thales CipherTrust Manager의 영구 무료 버전과 CipherTrust Data Protection Gateway 커넥터용 라이선스 3개, CipherTrust Transparent Encryption for Kubernetes 커넥터용 라이선스 3개를 제공합니다.

DPG(Data Protection Gateway)는 코드를 수정하지 않고도 레거시 및 클라우드 네이티브 애플리케이션에서 RESTful 호출을 사용해 민감한 데이터를 투명하게 보호하는 제품입니다. DPG는 데이터 보안 팀이 데이터를 보호하는 방법과 해당 데이터에 대해 액세스 권한을 갖는 사람, 데이터에 액세스할 수 있는 방법을 완벽하게 제어할 수 있게 해줍니다. 이와 동시에, 현재 환경에 손쉽게 통합이 가능하도록 DevOps에 조정이 쉬운 풀(pull) 및 배포 모델을 제공합니다.

CipherTrust Transparent Encryption for Kubernetes(CTE-K8s)는 승인된 사용자 및 프로세스를 결정하기 위해 정책 정의를 사용해 Kubernetes 파일 저장소의 민감 데이터를 투명하게 보호합니다. 권한 상승에 성공하더라도 정책 정의에 없는 사용자를 통한 위협 행위자는 상승된 권한을 행사할 수 없게 됩니다. 예를 들어, 랜섬웨어는 하드 드라이브의 데이터를 암호화하는데 CTE-K8s는 사용자 및 프로세스의 무단 읽기/쓰기를 금지하는 방법으로 파일을 보호하고, 이를 통해 랜섬웨어에 의한 스토리지 볼륨 내 파일의 손상/잠금/암호화를 방지합니다.

CipherTrust Manager는 조직이 암호 키를 중앙에서 관리하고, 보안 정책 및 액세스 제어를 세분화해서 구성 및 제어할 수 도와주는 업계 최고의 엔터프라이즈 키 관리 솔루션입니다. CipherTrust Data Security Platform의 기반이기도 한 CipherTrust Manager는 단일 플랫폼에 데이터 검색, 보호 및 제어를 하나로 통합한 데이터 중심의 통합 보안 제품군을 제공하는 CipherTrust 제품군의 중앙 관리 콘솔의 역할을 합니다.

주요 이점

멀티 클라우드 애플리케이션의 데이터를 투명하게 보호

Kubernetes 파일 저장소의 민감한 데이터를 투명하게 보호

완벽한 DevSecOps 업무 분장을 통해 효율성 향상

지원되는 사용 사례

CipherTrust Platform Community Edition은 DevSecOps 팀이 다음과 같은 사용 사례를 신속하게 구현할 수 있게 해줍니다.

- **앱 수준의 데이터 보호:** CipherTrust Data Protection Gateway를 통해 레거시 또는 클라우드 네이티브 애플리케이션에서 RESTful 호출을 사용해 민감한 데이터를 투명하게 보호
- **Kubernetes 파일 보호:** CipherTrust Transparent Encryption for Kubernetes를 통해 컨테이너나 Kubernetes 환경에 배포된 컨테이너에서 액세스할 수 있는 외부 스토리지 내부의 데이터를 투명하게 보호
- **키 관리:** 강력한 중앙 집중식 키 관리 및 암호화 솔루션인 CipherTrust Manager Community Edition에서 RESTful 호출을 사용해 애플리케이션을 보호

탈레스 소개

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

결단이 필요한 순간을 위한 결정적인 솔루션

CipherTrust Manager 기능	Community Edition	Enterprise Edition
REST API를 통한 키 관리	✔	✔
REST API를 통한 데이터 보호	✔	✔
외부 ID 공급자		✔
클러스터링		✔
멀티 도메인 지원		✔
내장형 또는 네트워크 HSM(Hardware Security Module)		✔
CipherTrust Data Security Platform 커넥터		
투명한 애플리케이션 보호	✔	✔
투명한 Kubernetes 환경 암호화	✔	✔
클라우드 키 관리		✔
데이터 검색 및 분류		✔
투명한 파일/폴더 암호화		✔
데이터베이스 보호		✔
애플리케이션 수준의 데이터 보호		✔
토큰화 - 볼티드, 볼트리스		✔
일괄적인 데이터 변환		✔

> cpl.thalesgroup.com <

문의처 – 모든 사무실 위치 및 연락처 정보는 아래 사이트를 참조 cpl.thalesgroup.com/contact-us