cpl.thalesgroup.com

THALES

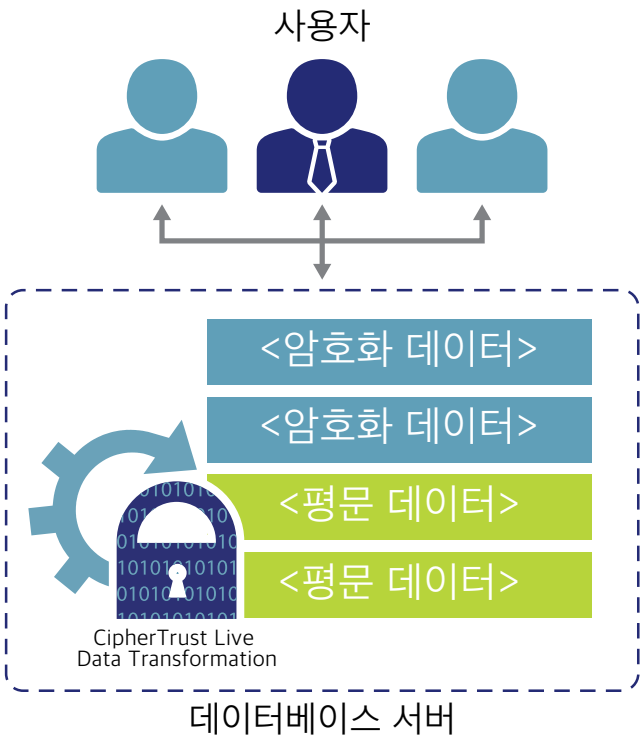
CipherTrust Live Data Transformation
무중단 암호화 및 키 교체

애플리케이션의 종료 없이 파일, 볼륨, Hadoop 환경에 암호화 및 접근 통제 적용

- 애플리케이션의 종료 없이 효과적인 암호화 및 접근 통제에 대한 규정 준수
- 애플리케이션 성능과 사용자에 미치는 영향을 최소화하면서 암호화 적용
- 무중단 암호화 및 키 교체로 암호화 환경 구현의 영향 및 비용 최소화
- 이전 키로 암호화된 데이터의 복구 시간 단축

직면 과제: 애플리케이션에 미치는 영향을 최소화하면서 암호화 구현 및 유지

보안 위협과 규정 준수 요구 사항이 날로 증가함에 따라 데이터 암호화는 IT 보안 전략의 계층화에 필수적인 요소가 되었습니다. 많게는 다음과 같은 두 가지 문제가 기존의 데이터베이스, 파일 및 빅데이터 환경에 암호화 기술을 도입하는 데 중대한 걸림돌로 작용합니다.



CipherTrust Transparent Encryption과 CipherTrust Live Data Transformation으로 보호된 데이터베이스는 무중단 초기 암호화 및 단순화되고 보다 유연한 암호키 교체를 가능하게 합니다. 암호화가 진행되는 동안 사용자는 평소와 같이 계속 작업할 수 있습니다.

- **초기 암호화 시간:** 대규모 데이터 세트를 보유한 경우, 초기에는 평문 데이터를 암호 데이터로 변환하려면 일반적으로 변환이 완료될 때까지 해당 데이터를 사용하는 애플리케이션을 종료해야 합니다. 최첨단 복제 및 동기화 기술을 사용하더라도 상당한 시간의 다운 타임이 불가피합니다. 상시 가용성을 요하는 업무용 애플리케이션의 경우, 이러한 가동 중단은 SLA 위반, 운영 중단, 매출 손실이라는 결과로 이어질 수 있습니다.
- **데이터 세트에 적용되는 키 교체로 인한 다운 타임:** 암호화된 데이터에 적용되는 키를 일정 주기마다 새 암호키로 변경해야 하는 경우가 종종 있습니다. 이를 위해서는 일반적으로 대규모 유지 관리 기간이 필요하며, 데이터를 처음 암호화할 때와 동일한 수준의 가동 중단이 발생합니다. 결과적으로, IT, 준법 및 보안 팀은 보안, 가용성, 가동 시간, 규정 준수 사이에서의 균형을 맞추기 위하여 어려운 결정에 직면하곤 합니다.

솔루션: CipherTrust Transparent Encryption용 CipherTrust Live Data Transformation 확장 모듈

고객들은 오랜 기간동안 CipherTrust Transparent Encryption에 의존해왔습니다. 기업에서 암호화를 구현하는 데 수반되는 문제 중 대다수는 CipherTrust Transparent Encryption로 해결 가능합니다. CipherTrust Transparent Encryption은 데이터 보안의 단절성 타파, 정형 데이터베이스와 비정형 데이터 암호화 지원, 전사적 중앙 집중화 키 관리 기능 제공 및 주요 SIEM(Security Information and Event Management) 시스템과 통합되는 사용자 접근 권한 통제 및 상세 데이터 접근 감사 로깅 기능을 지원합니다.

CipherTrust Transparent Encryption은 최소한의 가동 중단과 수고, 비용만으로도 실행 가능합니다. CipherTrust Transparent Encryption의 아키텍처를 통해 보안 팀은 애플리케이션, 네트워킹 또는 스토리지 아키텍처의 수정 없이 암호화를 구현할 수 있습니다.

CipherTrust Live Data Transformation은 이러한 이점 외에도, 고가용성, 복원성, 효율성 측면에서 특허받은 기술을 보유하고 있습니다.

서비스 중단없이 암호화를 구현하고 관리할 수 있는 특허받은 기능 지원

- **무중단 암호화 구현:** CipherTrust Live Data Transformation을 사용하는 관리자는 사용자, 애플리케이션 또는 워크플로우에 지장을 주지 않고 데이터를 암호화할 수 있습니다. 강력한 접근 통제 및 로깅 기능을 지원하므로 암호화가 진행되는 동안 데이터베이스 또는 파일 시스템을 정상적으로 사용할 수 있습니다.
- **중단 없는 암호 키 교체:** 보안 모범 사례와 다양한 규제 요건을 충족시키기 위해서 Live Data Transformation을 사용하는 기업은 데이터를 복제하거나 관련 애플리케이션을 종료하지 않고도 키 교체를 수행할 수 있습니다.

핵심 기능

CipherTrust Transparent Encryption 에이전트는 보안 및 제어해야 할 데이터를 저장하거나 접근하는 Windows 및 Linux 서버에서 작동됩니다. 실행하려는 서버에 에이전트용 라이센스를 적용하면 CipherTrust Manager에서 CipherTrust Live Data Transformation이 활성화됩니다. CipherTrust Live Data Transformation 라이센스는 언제든지 활성화할 수 있습니다. 라이센스가 활성화되면 사용자는 가동 중단이나 유지 관리에 시간을 허비할 필요 없이 곧장 업무 핵심 데이터를 안전하게 보호할 수 있습니다.

Live Data Transformation은 암호화 적용 규모 및 범위와 관계없이 애플리케이션과 사용자에게 암호화 작업의 투명성을 보장하는 기술을 제공합니다.

- **CPU 리소스 관리:** 대규모 데이터 세트를 암호화하려면 장시간 상당한 CPU 리소스가 필요할 수 있습니다. Live Data Transformation은 관리자가 암호화와 사용자가 의존하는 다른 CPU 작업에 리소스를 적절히 할당할 수 있는 정교한 CPU 관리 규칙을 제공합니다. 예를 들어 업무 시간 동안에는 암호화 작업이 시스템 CPU의 최대 10%를 소비하고, 나머지 90%는 어플리케이션을 위해 남겨두도록 리소스 관리 규칙을 설정할 수 있습니다. 그리고 CPU 리소스를 사용자가 많지 않은 야간과 주말에는 암호화가 70%를 사용할 수 있도록 설정할 수 있습니다. 또한 암호화 및 키 변경 프로세스는 수동으로 일시 중지하고 필요할 때 다시 재개할 수 있습니다.
- **버전 관리된 백업 및 아카이브:** CipherTrust Live Data Transformation은 백업 및 아카이브 데이터를 효율적으로 복구하여 즉시 사용할 수 있는 키 버전 관리 기능을 지원합니다. 데이터 복구 작업으로 CipherTrust Manager에서 복구된 아카이브용 암호키는 이전의 데이터 세트에 자동으로 적용됩니다. 복원된 데이터는 현재 암호키로 암호화됩니다.
- **복원성:** CipherTrust Live Data Transformation은 암호화 메타데이터를 대상 파일이나 데이터베이스 볼륨과 함께 저장하므로 스토리지 장애, 시스템 문제 또는 네트워크 가동 중단에도 뛰어난 복원력을 자랑합니다. 중단된 암호화 프로세스는 프로세스를 처음부터 다시 시작하지 않아도 원활한 복구가 가능합니다. 이 아키텍처는 오류가 발생한 원인, 시기 또는 위치와 관계없이 데이터 손상을 방지하며, 설계의 제약 없이 파일 시스템의 크기에 따라 확장할 수 있습니다.

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.