cpl.thalesgroup.com

THALES

CipherTrust Transparent Encryption

당면 과제: 변화하는 환경과 보안 위협 증가에 따른 민감 데이터 보안 방안

데이터 센터에서 운영 중인 데이터베이스와 파일을 보호하는 것만으로는 민감 데이터를 보호할 수 없습니다. 오늘날 대부분의 기업은 50가지 이상의 SaaS 애플리케이션과 빅데이터 환경, 컨테이너 기술, 그리고 자체 내부 가상 환경 및 프라이빗 클라우드와 더불어, 3개 이상의 IaaS 또는 PaaS 제공업체를 이용하고 있습니다.

설상가상으로, 사이버 공격은 갈수록 교묘해지고 강력해지고 있습니다. 민감 데이터의 보호에 관한 새로운 규정과 규제 지침이 잇따라 마련되고, 기존의 규제는 더욱 엄격해지고 있습니다.

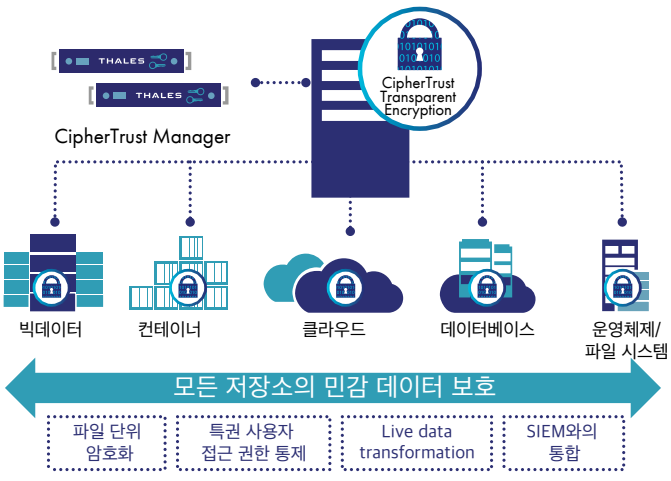
솔루션: CipherTrust Transparent Encryption

CipherTrust Transparent Encryption은 기업이 데이터 저장 위치와 관계없이 데이터 보호에 관한 규정을 준수하고 모범 사례를 따르는 데 유용한 중앙 집중식 키 관리, 사용자 접근 권한 통제, 세분화된 데이터 접근 감사 로깅 기능과 함께 저장 데이터 암호화 기능을 지원합니다. FIPS 140-2 인증을 받은 CipherTrust Transparent Encryption 에이전트는 운영 파일 시스템 또는 장치 계층에 상주하며, 이를 토대로 실행되는 모든 애플리케이션에 투명한 암호화 및 암호 해독 프로세스를 제공합니다. CipherTrust Transparent Encyption은 기업이 데이터에 접근할 수 있는 사람, 접근할 수 있는 시기, 부여되는 접근 등급을 결정할 수 있는 다양한 접근 통제 기능을 지원합니다.

모든 저장소의 민감 데이터 보호

- 파일, 볼륨, 클라우드 스토리지를 보호하는 동시에, 실제, 가상, 클라우드 환경에서 접근을 통제하고 데이터 접근 감사 로그를 제공하는 검증된 하드웨어 가속 암호화 솔루션을 사용하여 암호화, 접근 통제 및 데이터 접근 로깅에 관한 규정을 준수하며, 모범 사례 역시 참고할 수 있습니다.
- 다양한 유형의 클라우드, 온프레미스, 빅데이터 및 컨테이너 환경에도 간단하면서도 빠르게 확장 가능한 중앙 집중식 키 관리, 암호화, 접근 통제 정책을 적용할 수 있도록 지원합니다.
- 특권 사용자 접근 권한 통제 체제를 손쉽게 구현하여 관리자가 평소와 동일하게 근무하면서도 의심스러운 사용자의 데이터 접근을 차단할 수 있습니다.

CipherTrust Transparent Encryption



- 파일 접근에 대한 최고 수준의 분석 정보가 포함된 세부적이고 실효성 있는 보안 이벤트 로그를 활용하여 위협을 보다 빠르게 식별하고 차단할 수 있습니다.
- 업계에서 가장 다양한 플랫폼을 지원합니다. Linux, AIX 및 Windows 시스템에서 접근하는 정형 및 비정형 데이터를 보호하고, S3 스토리지에 저장된 데이터의 투명한 암호화와 접근 통제를 지원합니다.
- Live Data Transformation 옵션을 추가하여 중단 없이 암호화와 키 교체가 가능합니다. 여타 데이터 암호화 솔루션은 이와 같은 기능을 지원하지 않습니다.

주요 장점

투명한 데이터 보호: 애플리케이션, 인프라, 시스템 관리 작업 또는 업무 절차를 변경하지 않아도 파일 단위의 암호화를 지속적으로 실시하여 사용자와 프로세스의 무단 접근을 방지하고, 관련 접근에 대한 상세한 데이터 접근 감사 로그를 수집합니다.

원활하고 손쉬운 구현: CipherTrust Transparent Encryption 에이전트는 데이터가 저장되는 서버의 파일 시스템이나 볼륨 레벨에서 구현되며, 로컬 디스크뿐만 아니라 Amazon S3와 Azure Files 같은 클라우드 스토리지 환경도 지원합니다.

세분화된 접근 권한 지정 방식: 세분화된 최소 권한 사용자 정책을 적용하여 외부 공격이나 적법한 내부 사용자의 데이터 오용을 차단할 수 있습니다. 시스템, LDAP/액티브 디렉토리, Hadoop 및 컨테이너에서 사용자별, 그룹별 정책을 적용할 수 있습니다. 이 외에도 프로세스와 파일 유형, 날짜, 기타 변수에 따라 접근을 통제할 수 있습니다.

고성능 하드웨어 가속 암호화: CipherTrust Transparent Encryption 솔루션은 표준 기반의 강력한 암호화 프로토콜만을 사용합니다. 즉, 데이터 암호화에는 AES(Advanced Encryption Standard)를, 키 교환는 ECC(elliptic curve cryptography)를 사용합니다. 최신 CPU에서 지원되는 AES 하드웨어 암호화 기능을 사용하여 암호화 비용을 최소화할 수 있습니다.

포괄적 보안 분석: 상세 데이터 접근 감사 로그를 통해 위협을 빠르게 파악하여 차단함으로써 규정 요건을 준수할 뿐만 아니라, 데이터 보안에 대한 분석이 동시에 가능합니다. 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 활용됩니다.

다양한 시스템 및 환경 지원: 다양한 Windows, Linux 및 AIX 플랫폼에 에이전트가 적용될 수 있으며, 기본 스토리지 기술과 관계없이 실제, 가상, 클라우드, 컨테이너 및 빅데이터 환경에서 사용할 수 있습니다.

고급 보안

무중단 데이터 변환: Live Data Transformation 옵션을 추가하면 무중단 암호화와 키 교체가 가능합니다. 특허를 획득한 이 기술은 애플리케이션을 종료하지 않고도 데이터를 사용하는 동안 데이터베이스나 파일을 암호화하거나 새 암호키로 교체할 수 있습니다.

빅데이터(Hadoop)용 고급 접근 통제: Hadoop 환경에서 실행하는 경우 Hadoop 사용자와 그룹으로 접근 통제가 확대됩니다.

SAP HANA 인증: SAP는 데이터 암호화, 키 관리, 사용자 접근 권한 통제, 세분화된 파일 액세스 감사 로깅 기능을 지원하는 CipherTrust Transparent Encryption와 HANA v2.0의 호환성을 확인하였습니다.

CipherTrust Transparent Encryption UserSpace: Linux 서버에서 커널 업그레이드의 영향을 받지 않는 Linux FUSE 기반의 강력한 확장형 파일 암호화 솔루션입니다.

솔루션 아키텍처

본 솔루션의 아키텍처는 CipherTrust Transparent Encryption 에이전트와 CipherTrust Manager 어플라이언스로 구성됩니다. 정책과 키는 CipherTrust Manager에서 중앙 집중식으로 관리할 수 있습니다. CipherTrust Manager는 FIPS 140-2 레벨 1, 2 또는 3 인증을 획득한 어플라이언스로 제공됩니다.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption은 CipherTrust Data Security Platform에 포함되어 있습니다. CipherTrust 플랫폼은 데이터 식별, 분류, 보호 및 극도로 세분화된 접근 통제 기능을 중앙 집중식 키 관리 프로세스와 통합합니다. 따라서 데이터 보안 운영을 간소화하고, 규정을 준수하는 데 드는 시간을 절약하며, 클라우드 마이그레이션 절차를 보호하고, 전사적 위험 관리를 가능케 합니다. Thales CipherTrust Data Security Platform을 사용하면 자사의 모든 민감 데이터를 식별, 보호, 통제할 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.