

마이크로소프트 애저용 탈레스 솔루션



마이크로소프트 애저를 포함한 하이브리드에 위치한 워크로드 보안

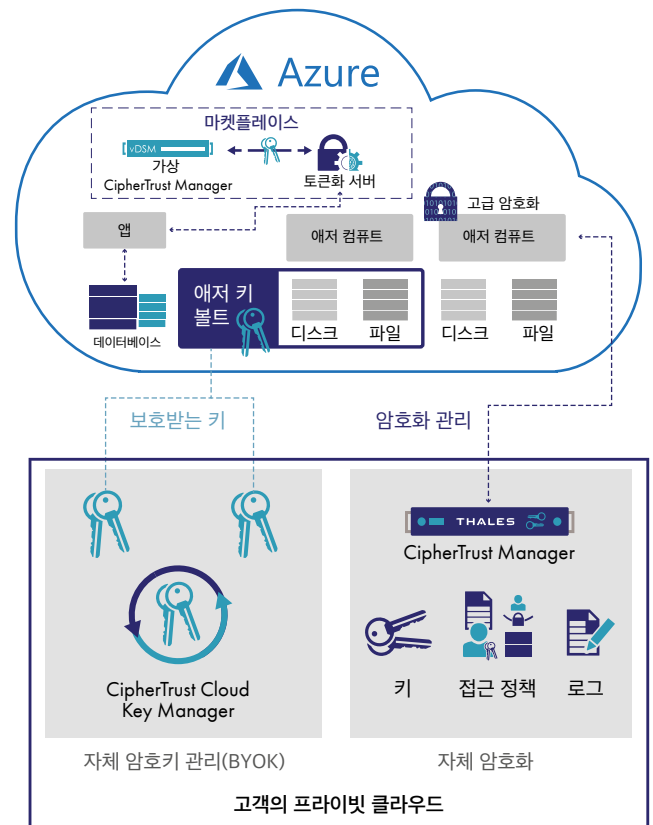
마이크로소프트 애저는 IT 워크로드를 편리하게 실행하고 비용을 절감할 수 있도록 지원합니다. 그러나 여전히 데이터 보호를 위한 최적의 운영 절차가 필요하고, 다양한 보안, 프라이버시 및 규제 요구사항을 준수해야 합니다. 게다가 현재 사용중인 모든 클라우드를 마이그레이션 할 경우를 대비한 신속한 데이터 이동성도 확보되어야 합니다. 만일, 특정 클라우드 벤더의 암호화 솔루션을 사용하게 된다면 이 기능이 약화될 수도 있습니다.

통합 키 관리 기능을 가진 고급 암호화 솔루션

효과적이고도 안전한 클라우드 사용에는 현재 증가하고 있는 민감데이터를 클라우드에서 사용하는 등의 매우 중요한 결정이 포함됩니다. 탈레스의 솔루션으로 효과적으로 디지털 트랜스포메이션을 보호하실 수 있습니다. 탈레스의 고급 암호화 및 중앙집중식 키 관리 솔루션은 구글 클라우드를 비롯한 다양한 클라우드 데이터를 위한 클라우드 저장데이터의 보안 및 제어기능을 제공합니다. 탈레스의 솔루션을 활용하면 다음과 같은 것들이 가능해 집니다.

- 암호화에 따른 중속성이 생기지 않습니다. 또한, 중앙집중식 독립 암호화 운영기능을 통해 구글 클라우드 플랫폼을 포함한 다양한 클라우드 환경에 위치한 데이터 및 워크로드를 효과적이면서도 안전하게 분산시킬 수 있어 데이터 이동성이 확보됩니다.
- 애저 키볼트를 활용하여 멀티 클라우드로 확장할 수 있는 중앙집중식 키 관리 기능이 가능합니다.
- 업계 선두의 SIEM 애플리케이션과 연계하여 데이터 액세스로그를 활용함으로써 보다 빠르게 공격을 감지합니다.

- 관리자 액세스 제어를 포함한 고급 암호화 기능을 제공하여 자격증명 손상으로 인한 위험을 감소시킬 수 있도록 지원합니다
- 볼트리스 토근화 솔루션과 연동하면 보안 기능을 갖춘 애플리케이션 설계가 가능합니다.



마이크로소프트 애저 및 기타 클라우드를 위한 고급 암호화 기능

IT 인프라가 100% 마이크로소프트 애저플랫폼 기반인데 엄격한 내부 또는 업계의 데이터 보안 규제를 준수해야 할 경우나 하이브리드 클라우드 기반이고 데이터가 기업 내 프라이빗 클라우드, 구글 클라우드 플랫폼 및 다른 클라우드 공급업체에 걸쳐 분산되어 있는 경우라면 고급 암호화 솔루션이 필요합니다. 구글 클라우드 플랫폼은 저장 데이터에 대한 암호화를 기본 기능을 제공하지만, 운영체제에는 평문 데이터를 제공하기 때문에 데이터가 OS수준에서 위험에 노출됩니다. CipherTrust Transparent Encryption은 구글 클라우드 플랫폼을 비롯 여러 곳에 저장되어 있는 파일과 데이터베이스를 보호합니다. 애플리케이션, 데이터베이스, 인프라 또는 비즈니스 절차, 그 어느 것도 바꿀 필요는 없습니다.

CipherTrust Transparent Encryption

- 사용자(루트 권한을 가진 관리자 포함), 프로세스, 파일유형, 시간 등을 포함하는 세부적인 최소 권한 사용자 액세스 정책을 기반으로 무단 액세스를 통제 함으로써 데이터 보안 강화
- 세부적인 파일 액세스 로그를 통해 규제 준수 요건 충족 및 침해 탐지 가속화. 다양한 SIEM 솔루션과 연동 가능
- 운영에 지장을 주지 않는 유연한 구현 및 신속한 투자 회수. 암호화 에이전트는 구글 컴퓨터 엔진 또는 스토리지에 액세스하는 기타 서버에서 실행되며 다양한 윈도우 및 리눅스 버전에서 사용 가능

중앙집중식 암호키 관리

CipherTrust Manager는 CipherTrust Transparent Encryption 및 Vormetric 토근화 서버에 대한 중앙화된 키, 정책 및 로그 관리를 제공합니다. DSM은 FIPS 140-2 레벨2 또는 3에 부합하는 물리적 어플라이언스나 FIPS 140-2 레벨1에 부합하는 가상 어플라이언스로 제공됩니다. 물리적 어플라이언스는 온프레미스에서 전 세계에 위치한 애저 컴퓨터 인스턴스 가상 머신 또는 기타 클라우드 공급업체에 걸쳐있는 암호화 에이전트를 관리하는데 적합합니다. 가상 어플라이언스는 VM웨어, KVM, AWS 및 마이크로소프트 애저에서 사용하실 수 있습니다.

PCI-DSS 규제 준수

마이크로소프트 애저용 [CipherTrust Tokenization with Dynamic Data Masking](#)은 데이터 센터, 빅데이터 또는 클라우드 환경의 데이터를 간소화하고 익명화 시킴으로써 PCIDSS 규제를 준수할 수 있도록 지원합니다. 형태보존 및 랜덤 토근화기능은 데이터베이스 구조를 유지하면서도 데이터의 민감한 필드를 보호할 수 있도록 지원합니다. 또한, 무중단 구현이 실현됩니다. 정책 기반 동적 데이터마스킹 기능의 경우 애플리케이션에 간단히 추가할 수도 있습니다

CipherTrust Tokenization Server는 마이크로소프트 애저 마켓플레이스에서 이용가능합니다.

멀티 클라우드 암호키 운영

[CipherTrust Cloud Key Manager](#)를 활용하면 조직의 외부에서도 업계의 모범사례를 따르며 자체 키 관리를 할 수 있습니다.

CipherTrust Cloud Key Manager는 클라우드 서비스 제공업체가 제공하는 자체키 관리(BYOK) API를 활용하여 암호키 관리의 복잡성을 감소시키는 한편, 중앙집중식 관리 및 가시성을 제공하여 운영효율성을 증대시킵니다. 본 솔루션은 마이크로 소프트 애저 마켓플레이스 또는 온프레미스에 설치 가능하며 보다 엄격한 규제 준수를 위해 프라이빗 클라우드에도 설치가능합니다.

CipherTrust Cloud Key Manager의 이점은 다음과 같습니다.

- 클라우드 혜택과 결합된 보다 안전한 키 관리, 경제적 비용 및 편의성
- 암호키에 대한 강력한 제어- 마이크로소프트 애저, 마이크로소프트 스택, 정부용 애저, 독일 및 중국용 애저 클라우드, AWS, KMS 등을 활용하여 직접 키를 생성, 저장
- 멀티 클라우드 키 관리 가능, 자동화된 키 교체, 단일 콘솔을 통한 포괄적인 키 수명주기 관리를 통해 IT운영 효율성 증대

데이터 보안 규제 요구사항 충족

탈레스는 마이크로소프트 애저 워크로드의 보안을 간소화시키고 데이터 보안 규제를 준수할 수 있도록 지원합니다. CipherTrust Transparent Encryption 및 토근화 솔루션은 애저 및 온프레미스 워크로드 및 암호키, 정책 등을 중앙에서 관리할 수 있도록 지원할 수 있도록 지원합니다. CipherTrust Cloud Key Manager는 클라우드 키 관리와 관련된 업계 모범사례 및 데이터 보안 규제를 준수할 수 있도록 지원합니다.

탈레스에 대하여

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한, 결정적인 기술.