클라우드 통합 옵션팩 (Cloud Integration Option Pack)

FIPS 140-2 HSM에서 암호화 키를 생성 및 제어한 뒤, 안전하게 클라우드로 내보내기

하이라이트

퍼블릭 클라우드 서비스 사용자에게 자신의 환경 내에서 암호화 키를 생성하고 이러한 키의 사용을 공유하면서도 필요한 만큼의 제어력을 유지하여 원하는 클라우드에서 사용할 수 있는 능력을 제공합니다.

- 멀티 또는 하이브리드 클라우드 전략을 지원하는 암호화 키 제어
- 강력한 엔트로피 소스를 활용한 안전한 키 생성
- FIPS 인증 HSM을 사용한 장기 키 보호
- 아마존 웹 서비스, 구글 컴퓨트 엔진, 마이크로소프트 애저 지원

최고 수준의 보증으로 클라우드에서 키 보호

브랜드와 데이터 보호

FIPS 140-2 및 공통 기준과 같은 최고 수준의 보안 표준에 따라 검증된 Entrust nShield HSM은 가장 어렵고 까다로운 보안 상황에서도 물리 서버 또는 클라우드의 데이터를 보호합니다.

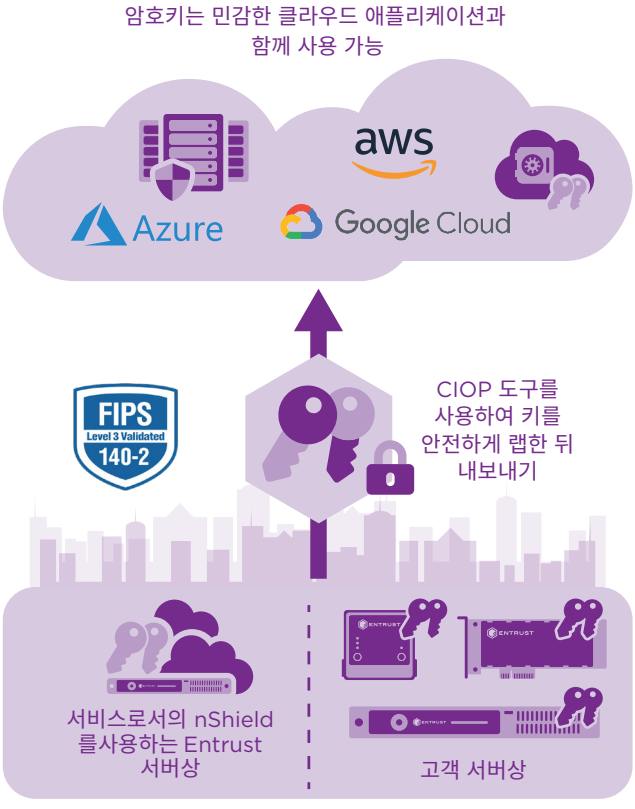

그림 1. 암호화 키는 nShield HSM에서 생성되어 랩 과정을 거치고 클라우드로 안전하게 내보내집니다

클라우드 통합 옵션팩 (Cloud Integration Option Pack)

지원되는 클라우드 서비스 제공업체

클라우드 통합 옵션팩(CIOP)은 nShield HSM을 사용해 암호화 키를 생성한 뒤 이를 랩하여 다음과 같은 클라우드 서비스 제공업체로 내보낼 수 있게 합니다.

- 아마존 웹 서비스(AWS)
- 구글 컴퓨트 엔진
- 마이크로소프트 애저 키 볼트(애저 BYOK 메커니즘 사용)

높은 수준의 보안을 찾는 고객에게 마이크로소프트에서 nCipher BYOK를 제공합니다. nCipher BYOK 방법은 생성 시점에서 만들어진 키 허가 사항이 마이크로소프트 애저 키 볼트로의 전송 종에도 유지되도록 추가적인 보증을 제공합니다. 또한, 마이크로소프트는 Entrust nShield Security World 사용해 특정 애저 지역 내 키 사용을 제한합니다. 이 방법은 CIOP를 구매하지 않아도 됩니다. 자세한 사항은 **키 볼트(nCipher)의 HSM 보호 키 가져오기** 를 참조하십시오.

하이브리드 및 멀티 클라우드 환경에서 키 제어

클라우드 통합 옵션팩은 하이브리드 클라우드 전략, 단일 클라우드 서비스 제공업체 도는 멀티 클라우드 전략과 상관 없이 고객에게 필요한 제어와 보증을 제공합니다. 암호화 키를 클라우드 서비스 제공업체로 가져옴으로써 한 클라우드 서비스 제공업체에서 다른 제공업체로 이전하는 것을 어렵게 만드는 업체 종속에 따르는 어려움을 예방합니다.

지원 구성

- 애저 BYOK 관련 nShield 시큐리티 월드 소프트웨어 v12.60 및 펌웨어 v12.60 또는 그 이상 요구
- AWS 및 구글 컴퓨트 엔진 관련 nShield 시큐리티 월드 소프트웨어 v12.40 소프트웨어 요구
- 본 출시품은 다음을 포함한 다양한 플랫폼에서 호환성 테스트를 거쳤습니다.
  - **마이크로소프트 윈도우 서버** 2019 x64 **및** 2016 x64
  - **마이크로소프트 윈도우** 10 x64 **및** 7 x64
  - Red Hat Enterprise **리눅스** 7 x64 **및** AS/ES 6 x86/x64
  - SUSE Enterprise **리눅스** 12 x64 **및** 11 x64
  - Oracle Enterprise **리눅스** 7.6 x64 **및** 6.10 x64
- 지원 HSM
  - **모든 현재** nShield **모델과 호환 가능**

자세히 보기

Entrust nShield HSM에 대해 더 알아보시려면 **entrust.com/HSM**을 방문하십시오. 신원, 접근, 소통 및 데이터에 관련된 Entrust의 디지털 보안 솔루션에 대해 더 알아보시려면 **entrust.com**을 방문하십시오.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com