Microsoft와 Entrust, 독자적인 BYOK 솔루션으로 클라우드 보안과 신뢰 증진

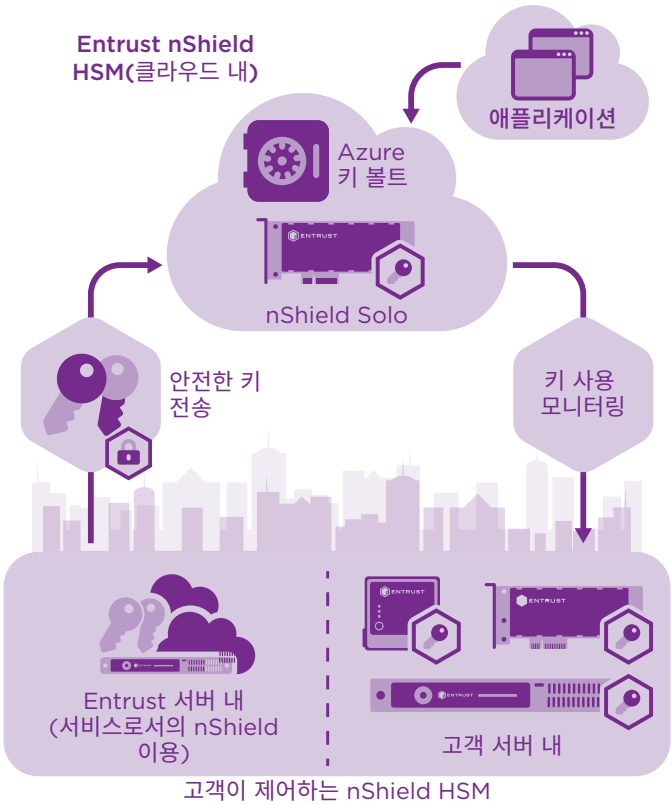
Microsoft Azure Key Vault와 Entrust nshield HSM으로 클라우드 내 중요 데이터와 키에 대한 통제권 확보

하이라이트

- FIPS 140-2 인증 환경에서 키 보호
- 클라우드 내 애플리케이션에서 키 확인이 불가능하도록 보장
- 애플리케이션과 키 관리 기능 분리
- 암호키와 애플리케이션 기밀에 대한 정밀한 제어 가능
- 사용하는 만큼 지불하는 서비스로 빠른 확장 가능

문제: 일반적으로 통제권 확보를 기대할 수 없는 퍼블릭 클라우드 서비스

공유 서비스로서의 퍼블릭 클라우드 인프라에서는 테넌트 실행이나 저장 공간에 대한 구분이 항상 명확하지는 않습니다. 클라우드 서비스 공급업체는 암호화를 사용하여 액세스를 제어하고 민감한 데이터의 기밀성과 무결성을 보호합니다. 그러나 서비스의 보안은 암호키에 부여하는 보호 수준에 따라 달라지며 노출 시 민감한 데이터가 훼손될 수 있습니다.



Entrust nShield HSM을 사용하면 고객이 자체적으로 키를 생성하고 사용하며 클라우드 내 데이터를 보호할 수 있습니다.

독자적인 BYOK 솔루션으로 클라우드 보안과 신뢰 증진

과제: 민감한 데이터를 보호하는 암호키의 통제권 유지

클라우드 서비스는 필요에 따라 신속하게 배포하고 확장할 수 있습니다. 이러한 환경에서 데이터를 보호하려면 클라우드 애플리케이션에서 사용하는 암호키를 제어해야 합니다. 암호키와 애플리케이션 기밀에 대한 통제권을 유지하는 것은 퍼블릭 클라우드 서비스의 신뢰도와 견고성을 높이는 데 필수적입니다.

솔루션: Entrust nShield HSM으로 보강한 키 제어 기능을 포함하는 Microsoft Azure Key Vault

Microsoft Azure Key Vault는 클라우드에서 고유한 보안 컨테이너를 생성하는 기능을 제공합니다. Entrust nShield® 하드웨어 보안 모듈(HSM)로 민감한 데이터와 키를 보호하고 관리하는 Microsoft Azure Key Vault를 사용하면 통제권을 유지할 수 있습니다. Entrust nShield HSM은 클라우드의 소프트웨어 환경과 관계없이 암호키를 보호합니다. 클라우드에서 실행하도록 승인받은 애플리케이션은 키를 사용할 수 있지만 볼 수는 없습니다.

BYOK(Bring Your Own Key) 옵션을 사용하면 고객이 자체적으로 Entrust nShield HSM을 사용하여 Microsoft에서 보유한 클라우드의 HSM에 안전하게 키를 생성하고 전송할 수 있습니다. Microsoft는 키의 캐시 복사본을 받게 되며 Azure 내에서 적합하게 승인받은 애플리케이션에서 키를 사용할 수 있습니다. 재해 복구를 위해 HSM간에 키를 복제할 수 있지만 하드웨어가 HSM 외부에서 키를 보는 것을 허용하지는 않습니다. BYOK는 nShield 'Security World'로 알려진 인증받은 보안 범위 내에서 잠금 상태로 키를 유지합니다. 실시간에 가까운 사용 로그를 통해 Azure에서 키를 사용하는 방법과 시점을 정확하게 확인할 수 있어 추가 보안을 제공합니다. 키 소유자는 키 사용을 모니터링하고 필요한 경우 키 액세스를 취소할 수 있습니다.

Entrust HSM을 Microsoft Azure Key Vault와 함께사용해야 하는 이유

Entrust nShield HSM은 클라우드에서 민감한 데이터를 보호하는 암호키를 안전하게 관리합니다. Entrust nShield HSM 기능:

- Security World에서 생성한 보안 범위를 내에서 암호키를생성하고 안전하게 전송
- FIPS 140-2 인증 암호화 범위 내에서 Microsoft가 보유한 키에 보호 제공
- 강력한 액세스 제어 메커니즘과 역할 분리 시행을 통해 암호키를 언제든지 사용할 수 있으며 승인된 목적으로만 사용하도록 보장

독자적인 BYOK 솔루션으로 클라우드 보안과 신뢰 증진

고보장성 클라우드 보안

Entrust nShield HSM은 공유 보안 인프라를 가진 공유 서비스라는 클라우드의 한계 때문에 클라우드에 보관하는 민감한 데이터가 취약하다는 인식을 불식시킵니다. Entrust nShield HSM 기능:

- 강력한 변조 방지 환경에서 키 보안
- 행정 업무에서 보안 기능을 분리하여 보안 정책 집행 가능
- 공공 부문, 금융 서비스,기업 관련 규제 요건 준수

Entrust HSM

Entrust nShield HSM은 현재 이용 가능한 솔루션 중에서도 최고 성능을 갖추었으며 가장 안전하고 통합하기 쉬운 HSM 솔루션 중 하나로, 규정 준수를 촉진하고 기업, 금융 기관과 정부 기관에 최고 수준의 데이터 보안과 애플리케이션 보안을 제공합니다.

Entrust만의 Security World 키 관리 아키텍처를 이용하면 강력하고 세분화된 방식으로 키 액세스와 사용을 통제할 수 있습니다.

Microsoft

Microsoft는 기업들이 애플리케이션을 운영하고, 콘텐츠를 생성하고 공유하며 공동 프로세스를 구축하는 방식을 혁신했습니다. Microsoft Azure Key Vault를 기반으로 하는 시스템을 이용하면 클라우드 서비스에 더욱 안전하게 액세스할 수 있습니다. Microsoft Azure Key Vault는 암호화를 차용하여 데이터를 보호하고, 신뢰할 수 있는 비즈니스 환경을 구축하며 이렇게 구축된 환경은 다음과 같은 이점을 제공합니다.

- Active Directory에 대한 앵커로서 데이터와 키에 대한 통제권 유지 가능
- 빠르고 확장 가능한 배포와비용 효율성 등 클라우드에 대한기대 충족
- 애플리케이션 관리와 키 관리 사이의 역할 분리 지원

관련 링크

entrust.com/HSM을 방문하면 Entrust nShield HSM에 관해 자세히 알아보실 수 있습니다. **entrust.com**을 방문하면 Entrust의 신원, 접근, 통신, 데이터 관련 디지털 보안 솔루션에 관해 자세히 알아보실 수 있습니다.

Microsoft Partner
Microsoft
Gold Application Integration
Gold Datacenter

Entrust nShield HSM
관련 정보 확인 및 문의

HSMinfo@entrust.com

entrust.com/HSM

ENTRUST CORPORATION 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명도 넘는 동료, 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기:
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com