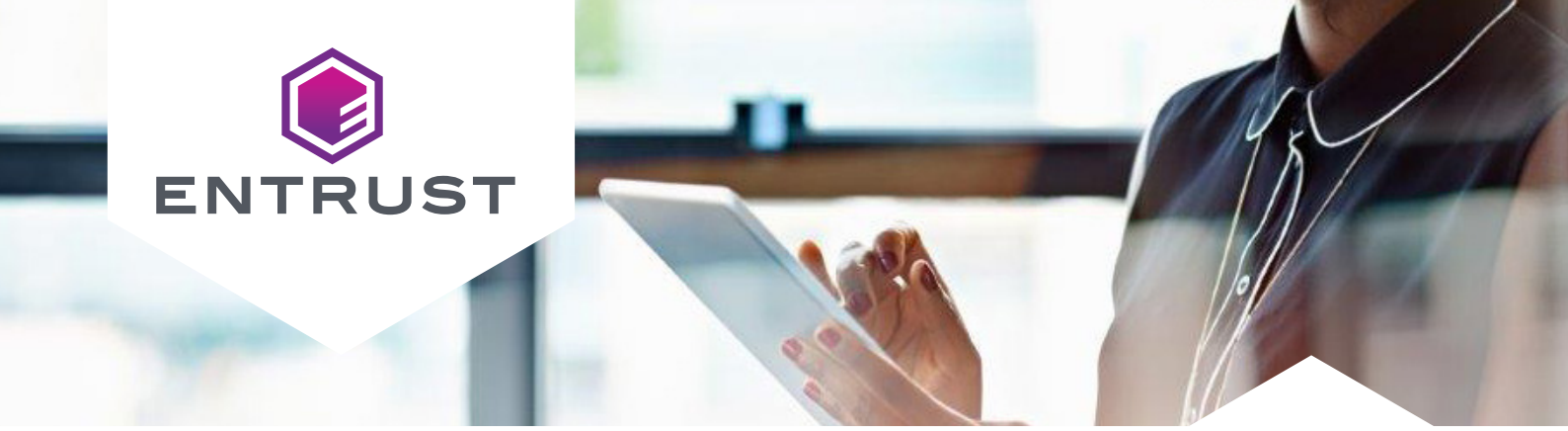

nShield 데이터베이스 보안 옵션 팩

Microsoft SQL 서버 데이터베이스와 고신뢰성 nShield 하드웨어 보안 모듈과의 원활한 통합

하이라이트

Microsoft SQL 서버 데이터베이스 배포에 대한 강력한 신뢰점

- 모범 사례 FIPS 및 공통 기준 인증 하드웨어 보안 모듈(HSM)에서 데이터베이스 암호화 키 보호
- 셀 수준 암호화 및 투명 데이터 암호화(TDE) 모두 보호
- 조직의 중요 데이터를 침해로부터 보호

데이터베이스는 대부분의 조직에서 중요한 정보의 보고입니다. 기업 데이터베이스는 고객의 신용카드 데이터, 기밀 정보, 지적재산권이 포함되어 있습니다. 분실 또는 도난된 데이터는 조직에게 상당한 평판 및 브랜드 손상의 위험뿐만 아니라 심각한 벌금의 부담도 지게 합니다. 조직의 내외부 위협으로부터 중요한 데이터를 보호함으로써 조직은 데이터 침해의 위험을 완화하고 신용카드 데이터 보안 인증(PCI DSS)을 포함한 규제 및 입법 규정을 준수합니다. 실로 최신 PCI DSS 표준(v3.2.1)의 3.6항은 “암호화 키는 안전하게 저장되어야 한다...HSM과 같은 보안 암호화 장치 내에서”라고 명시하고 있습니다. 또한 3.6항은 이중 제어와 같은 HSM의 기능으로 제공되는 키 관리 모범 사례를 개략적으로 설명합니다.

최고 수준의 신뢰성으로 데이터베이스 보호

데이터베이스의 데이터를 암호화하면 데이터가 보호되지만 데이터의 잠금을 해제하는 암호화 키 또한 보호되어야 합니다. 하드웨어 보안 모듈(HSM)을 사용하면 안전하고 신뢰할 수 있는 플랫폼에 키를 데이터와는 별도로 저장함으로써 암호화 키를 보호할 수 있습니다. nShield HSM은 역할 기반 인증을 요구하고 보안과 데이터베이스 관리를 분리하여 내부 보안 정책을 실행하고 감사자에게 규정 준수를 보다 쉽게 증명할 수 있도록 합니다.

단일 서버 전용 PCIe 카드나 가상화 환경을 위한 공유 네트워크 어플라이언스로 사용 가능합니다.

SQLEKM 제공자로도 알려진 nShield 데이터베이스 보안 옵션 팩(Microsoft SQL 서버용)은 Microsoft SQL 서버를 위해 제공되는 확장 가능한 키 관리(EKM) API입니다.

nShield 데이터베이스 보안 옵션 팩

Microsoft SQL 서버에는 데이터를 보호하기 위한 TDE와 셀 수준 암호화라는 두 가지 암호화 기능이 내장되어 있습니다. 이러한 기능을 통해 데이터베이스 전체를 보호하거나 중요한 데이터베이스 필드만 선택적으로 보호할 수 있으며, 기존 애플리케이션, 데이터베이스 구조 및 프로세스를 방해하지 않고도 활성화할 수 있습니다.

브랜드와 데이터 보호

FIPS 및 공통 기준과 같은 최고 수준의 보안 표준에 따라 검증된 Entrust nShield HSM은 가장 어렵고 까다로운 보안 상황에서도 데이터를 보호할 준비가 되어 있습니다. nShield HSM의 소단위 접근 제어를 통해 Microsoft SQL 서버용 암호화 키를 관리할 수 있습니다. 정책을 시행하기 위해 보안 기능은 관리 기능으로부터 분리됩니다.

Entrust nShield HSM은 다음을 제공합니다.

- **하드웨어 키 보호** – 데이터베이스 암호화 키를 안전한 변조 방지 환경에 저장하여 복사 또는 손상을 방지
- **사용자 및 역할 시행** – Microsoft SQL 서버에서 암호화된 데이터베이스에 접근하기 위한 보다 강력한 제어 기능 제공
- **엄격한 키 제어** – 관리자의 스마트 카드 인증을 사용하여 데이터베이스 암호화 키에 대한 강력한 제어 기능 제공
- **역할 분담** – 여러 관리자에 걸쳐 중요한 작업 및 절차에 대한 책임 분담
- **간편한 설정 및 통합** – Entrust nShield HSM은 Microsoft SQL 서버와 원활하게 통합되어 다음과 같은 이점을 제공합니다.
  - 해당 암호화 키의 보호를 포함한 TDE 및 셀 수준 암호화 모드

변화하는 요구사항에 맞게 확장 가능한 nShield HSM은 웹 및 애플리케이션 서버, 공용 키 인프라(PKI)를 비롯한 다른 주요 기업 애플리케이션과 즉시 통합됩니다.

네트워크 기반 nShield 커넥트 HSM은 여러 서버에서 공유되어 다음과 같은 기능을 제공할 수 있습니다.

- **가상화 환경 지원** – Hyper-V 및 VMware를 포함한 가상화 서버를 위한 하드웨어 기반 키 스토리지
- **페일오버 클러스터 지원** – AlwaysOn 가용성 그룹 포함
- **간소화된 관리** – 다수의 데이터베이스의 암호화 키에 더불어 다른 애플리케이션에서 사용하는 키 관리
- **페일오버 기능** – 높은 가용성이 중요한 경우 HSM을 사용할 수 없게 되면 사용자에게 자동으로 다른 HSM으로 전환할 수 있는 옵션 제공
- **재해 복구** – 키 아카이브 및 복구를 위한 간단하고 안전한 프로세스
- **비용 효율적인 리소스** – 여러 서버에서 모듈을 공유하여 사용함으로써 하드웨어, 라이선스 및 운영 비용 절감

nShield 데이터베이스 보안 옵션 팩

기술 사양

지원 구성

- nShield 시큐리티 월드 소프트웨어 v12.40.2 또는 v12.60.x 이상.
- Microsoft SQL 서버 버전(기업 에디션) 2019 x64, 2017 x64
- Windows 서버 운영 체테 지원 2019 R2 x64, 2016 R2 x64
- 지원 HSM
  - 모든 nShield 솔로 및 커넥트 HSM 모델과 호환 가능

지원하는 암호화 알고리즘

- 비대칭 - RSA 2048, 3072 및 4096 비트 키 길이 포함
- 대칭 - AES 128, 192 및 256 비트 키 길이 포함

지원 NSHIELD 기능

nShield HSM을 Microsoft SQL 서버와 통합하여 다음과 같은 기능을 이용하십시오.

기능	지원
1 of N 카드 세트	예
K of N 카드 세트	아니요
소프트카드	예
모듈 제한 키	아니요
키 복구	예
키 가져오기	부분[1]
로드 밸런싱	예
페일오버	예
엄격한 FIPS(FIPS 140-2 레벨 3) 지원	예[2]

1. 키 가져오기는 nCore 키에 대해서만 지원됩니다. nCore API는 nShield 모듈을 위한 기본 애플리케이션 프로그래밍 인터페이스입니다 2. 자세한 내용은 출시 정보 및 사용자 안내서를 참조하십시오.

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.

Entrust nShield HSM에 대해 더 알아보시려면

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 신뢰받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

연락처:
HSMinfo@entrust.com