

비센스바움 보안 제품 소개서

- 하드웨어 보안 모듈 - HSM
- 데이터 암호화 솔루션 – CipherTrust Data Security Platform
- 암호 키 관리 솔루션 – Data Security Manager



I 하드웨어 보안 모듈 HSM 소개

하드웨어 보안 모듈(HSM)은 고객의 데이터를 암호화 하는 키와 디지털 서명 및 인증서를 생성 하여 암호화 프로세스를 제공하는 강력한 전용 하드웨어 장치입니다. Thales의 암호화 기술로 고객의 중요한 키를 관리하고, 변조방지 기술로 키의 변조를 방지하는 기능을 갖춘 네트워크 연결 기 기입니다. HSM은 보관하고 있는 암호화 키를 외부로 반출하지 않기 때문에 최고 수준의 보안을 제 공합니다.

I 하드웨어 보안 모듈 HSM 제품 구성

Luna Network HSM



Luna Network HSM은 온프레미스, 가상 및 클라우드 환경의 애플리케이션에서 사용하는 암호키를 보호하는 네트워크 연결 HSM입니다. Luna Network HSM은 시장에서 가장 빠르고 가장 안전한 HSM입니다. 여러 애플리케이션 또는 사업 부가 공통 HSM 플랫폼을 공유할 수 있어 투자 수익이 증가합니다.

Luna PCIe HSM



임베디드 HSM인 **Luna PCIe HSM**은 암호키와 민감한 암호화 작업을 보호합니 다. 전용 성능 또는 애플리케이션 보안 사용 사례를 위한 이상적인 솔루션입니 다.

Luna USB HSM



Luna USB HSM은 오프라인 키 저장 장치에 루트 암호키를 저장하는 데 이상적 인 USB 연결 HSM입니다. PKI 루트 키 보호와 같은 오프라인 솔루션에 이상적입 니다.

I 하드웨어 보안 모듈 HSM 주요기능

- ❖ 키 탈취 변조 차단
 - 암호화 키를 전용 하드웨어에 저장하여 키 탈취나 변조를 차단
- ❖ 표준 암호화 관련 API 제공
 - PKCS#11, Java(JCA/JCE), Microsoft CAPI 및 CNG, OpenSSL
- ❖ 강력한 사용자 권한
 - 모든 암호화 작업이 HSM내에서 이루어지기 때문에 강력한 사용자 권한에 의한 액세스 제어
- ❖ 이중화 구성
 - 이중화 구성 및 자동 Sync 지원
- ❖ 보안 관련 국제 표준 인증 및 법적 규제 요건 충족
 - FIPS 140-2, CC EAL 4+, PCI-DSS, GDPR 등

I 하드웨어 보안 모듈 HSM 장점

- ❖ 빠른 처리 속도
 - 초당 20,000 이상의 ECC 및 10,000 이상의 RSA 작업 성능으로 짧은 대기시간 및 인적/물적 리소스 감소
- ❖ 컴플라이언스 준수
 - FIPS 140-2 Level 3 인증, GDPR, eIDAS, HAPPA, PCI-DSS 규제 준수
- ❖ 확장성과 유연성
 - 100개의 암호로 격리된 파티션 분리되어 독립적인 HSM처럼 작동
- ❖ Root of Trust
 - 수백개의 독립된 어플리케이션의 암호화 키 보관/수명주기 보호
- ❖ 효율성
 - HSM 원격 관리로 이동 불필요 / 멀티 테넌트로 HSM 공유를 통한 리소스의 효율적인 처리

I 하드웨어 보안 모듈 HSM 제품 사양

- ❖ 각 모델별 시리즈를 선택할 수 있습니다.
- LUNA HSM A 시리즈 : 손쉬운 관리를 위한 비밀번호 인증 타입

Luna A Series:

Password Authentication for easy management.

Standard Performance A700	Enterprise Performance A750	Maximum Performance A790
Up to 4 MB Memory Partitions: 5 Maximum Partitions: 5	Up to 32 MB Memory Partitions: 5 Maximum Partitions: 20	Up to 64 MB Memory Partitions: 10 Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

- LUNA HSM S 시리즈 : 높은 보증 사용 사례를 위한 멀티 팩터 인증 (PED 타입)

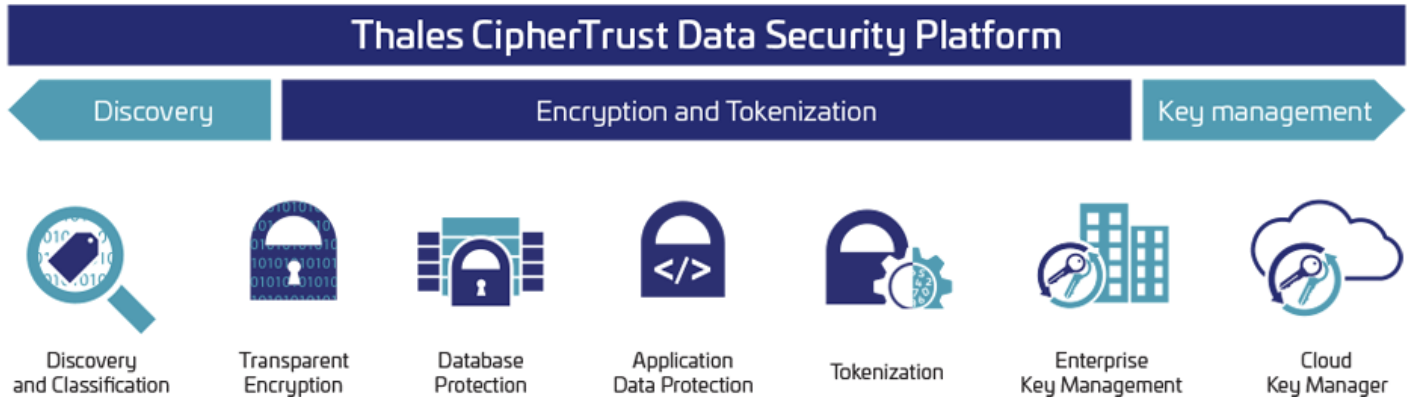
Luna S Series:

Multi-factor (PED) Authentication for high assurance use cases.

Standard Performance S700	Enterprise Performance S750	Maximum Performance S790
Up to 4 MB Memory Partitions: 5 Maximum Partitions: 5	Up to 32 MB Memory Partitions: 5 Maximum Partitions: 20	Up to 64 MB Memory Partitions: 10 Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

I 데이터 암호화 솔루션 소개

데이터를 물리적 데이터센터, 프라이빗 또는 퍼블릭 클라우드, 타사 스토리지 애플리케이션 등 어디에 보관하든 상관없이 중요한 데이터를 보호하려면 적절한 암호화와 키 관리가 필수입니다. 탈레스는 데이터베이스, 애플리케이션, 파일 및 스토리지 컨테이너에 저장된 정형·비정형 데이터를 대상으로 세분화된 암호화, 토큰화, 역할 기반 액세스 제어 기능을 지원하는 저장 데이터 암호화 솔루션을 제공합니다. 중앙 집중식 키 관리, 강화된 신뢰성으로 기업은 마스터키를 보호하고 데이터 안전을 지킬 수 있습니다.



I 데이터 암호화 솔루션 장점

- ❖ 운영 단순성
 - 중앙집중식 정책, 암호키 관리는 기업 안팎의 모든 물리·가상 서버에서 데이터 제어를 보장합니다.
- ❖ 위험 최소화
 - 확장 가능한 고성능 데이터 암호화로 데이터 보안 관련 규제를 준수하고 모범 사례 요건을 충족하여 외부 위협이나 악의적인 내부자에게서 데이터를 보호할 수 있습니다.
- ❖ 보안 민첩성
 - 준비된 솔루션으로 모든 중요 데이터를 보호하여 새로운 데이터 보안 요건과 규정 준수 요건에 신속하게 대응합니다.



키 관리

접근 정책 관리

감사 보고서



유연한 API



FIPS 140-2 Compliant



- 중앙 집중화된 키 관리 및 역할 기반 정책에 따른 통제
- 자사의 다양한 암호화 제품의 통합 관리 기능
- 다양한 로그 포맷 지원을 통해 향상된 감사 및 보고서 기능, 맞춤형 경보 기능
- 자동화된 암호화 및 관리 기능 구현을 위해 다양하고 유연한 REST API 지원
- 강력한 역할 분리(separation of duties) 와 Multi-tenant 지원
- 물리적 어플라이언스 또는 가상머신 형태로 제공
HSM 내장 또는 연동을 통해 FIPS 140-2 L 3 지원

I 데이터 암호화 솔루션 제품 구성

CIPHERTRUST DATA SECURITY DATA PLATFORM

차세대 통합 데이터 보호 서비스로 어디서나 조직의 민감한 데이터를 검색, 보호하고 제어할 수 있습니다.

CIPHERTRUST MANAGER

업계 최고의 엔터프라이즈 키 관리 솔루션을 제공하여, 암호키를 중앙에서 관리하고 보안정책을 구축할 수 있도록 지원합니다.

CIPHERTRUST TRANSPARENT ENCRYPTION (CTE)

파일, 디렉터리, 볼륨에 대한 고성능 암호화와 최소한의 권한 액세스 제어를 제공합니다.

DEVSECOPS-FRIENDLY DATA PROTECTION

API를 통해 키 관리, 서명, 해싱, 암호화 서비스와 같은 암호화 기능을 제공합니다.

CIPHERTRUST TOKENIZATION

토큰화, 동적 데이터 마스킹을 기존 애플리케이션에 신속하게 추가하여 데이터를 보호하고 규정을 충족합니다.

CIPHERTRUST DATABASE PROTECTION (CDP)

포괄적인 암호화, 세분화된 제어를 제공하여 데이터베이스 환경에서 가장 민감한 데이터를 보호합니다.

CIPHERTRUST BATCH DATA TRANSFORMATION (BDT)

고속 보안 데이터 마스킹

CIPHERTRUST CLOUD KEY MANAGER (CCKM)

여러 클라우드 공급업체가 암호화한 데이터의 암호키와 정책을 강력하게 제어할 수 있습니다.

ENTERPRISE ENCRYPTION KEY MANAGEMENT

타사 장치, 서버, 데이터베이스, 저장소, 가상 환경을 위한 일원적인 키 관리

I 데이터 암호화 솔루션 활용 사례

❖ 규제준수

- 강력한 관리 정책을 통한 암호화, 접근제어, 로그, FIPS 140-2의 1, 2, 3레벨 및 CC인증(공통 평가 기준)을 준수하는 암호키 관리는 각종 규제 및 규정을 효과적으로 준수할 수 있도록 지원합니다.

❖ 클라우드 보안

- 암호화와 키 관리를 통해 데이터를 통제하면서, 업무를 클라우드와 호스트 된 환경으로 안심하고 이동시킬 수 있습니다.

❖ 데이터베이스 보안

- 다양한 데이터베이스와 빅데이터가 혼재하는 환경에서 보안 감사 로그를 수집하고, 사용자 접근 권한을 제어하고, 암호화합니다.

I 암호 키 관리 솔루션 소개

암호 키 관리 제품은 클라우드 환경과 엔터프라이즈 환경에서 다양한 사용 사례에 대한 키 관리 작업을 간소화하고 강화합니다. FIPS 140-2 준수 가상·하드웨어 장치를 활용하는 탈레스 키 관리 도구와 솔루션은 민감한 환경에 수준 높은 보안을 제공하고 자체 암호화, 타사 애플리케이션의 키 관리를 일원화합니다. 따라서 데이터 보안을 강화하는 동시에 더 강력한 키 통제력을 확보할 수 있습니다. 탈레스 키 관리 제품은 표준 인터페이스를 통해 애플리케이션과 연결 가능하며, 강력한 키 관리 기능을 제공합니다.

I 암호 키 관리 솔루션 장점

❖ 민감한 데이터를 위한 철저한 보안

- 탈레스 엔터프라이즈 키 관리 제품은 FIPS 140-2 준수 가상·하드웨어 장치를 활용하여 데이터 보호에 필요한 강력한 보안 암호키를 생성, 제공, 보관합니다. CipherTrust 매니저는 하드웨어나 가상 장치로 사용할 수 있습니다.

❖ 비용 간소화 및 절감

- 탈레스 키 관리 소프트웨어 솔루션은 다양한 암호화 환경의 키 관리를 일원화하는 단일 창을 제공하여 여러 공급업체를 소싱할 필요 없이 단순성을 누리고 비용을 절감할 수 있습니다. 더 강력한 키 구성으로 데이터 보안을 강화하는 동시에 키 통제력을 강화하는 통합 솔루션입니다.

❖ 키 통제력 강화

- 엄격한 키 정책 시행이나 세분화된 액세스 제어, 자체 키 소스를 사용하여 키를 생성하고 클라우드·엔터프라이즈 애플리케이션으로 내보내는 등, 탈레스 엔터프라이즈 키 관리 제품을 사용하면 암호키를 통제할 수 있습니다.

중앙 집중 키관리 매니저



키 관리



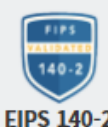
접근 정책 관리



감사 보고서



유연한 API

FIPS 140-2
Compliant

CipherTrust Manager

중앙 집중화된 키 관리 및 역할 기반 정책에 따른 통제

자사의 다양한 암호화 제품의 통합 관리 기능

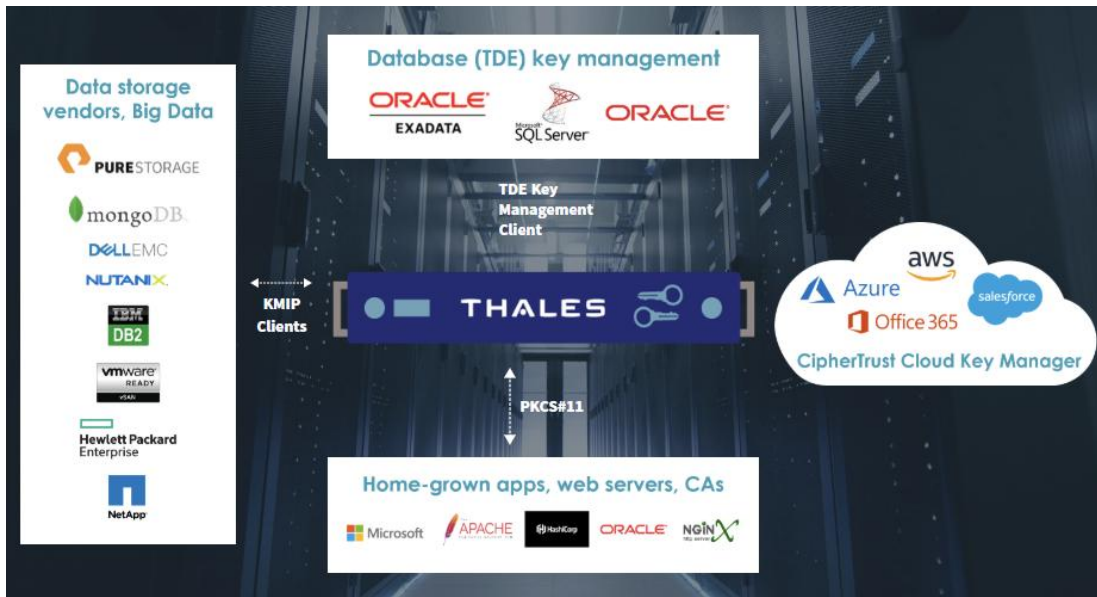
다양한 로그 포맷 지원을 통해 향상된 감사 및 보고서 기능, 맞춤형 경보 기능

자동화된 암호화 및 관리 기능 구현을 위해 다양하고 유연한 REST API 지원

강력한 역할 분리(separation of duties)와 Multi-tenant 지원

물리적 어플라이언스 또는 가상머신 형태로 제공
HSM 내장 또는 연동을 통해 FIPS 140-2 L3 지원

I 암호 키 관리 적용 범위



I 암호 키 관리 솔루션 제품 구성

CipherTrust Manager

CipherTrust Manager는 FIPS 준수 가상·물리 장치 제품 형태로 사용할 수 있는 중앙 집중식 키 수명 주기 관리 기능과 정책 제어 기능을 제공합니다.

Data Security Manager

Vormetric 데이터 보안 관리자는 데이터 보안 관리 콘솔로 중앙 집중식 정책·암호키 관리를 지원하는 데이터 보안 장치입니다.

CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager는 멀티 클라우드, 하이브리드, 엔터프라이즈 환경에서 키 수명 주기 관리를 일원화합니다.

Enterprise Key Management

엔터프라이즈 키 관리 솔루션은 데이터베이스 TDE, KMIP 클라이언트, 탈레스 데이터 보안 플랫폼 솔루션을 포함한 여러 애플리케이션을 대신하여 키를 관리하고 보호합니다.

I 암호 키 관리 솔루션 활용 사례

❖ IaaS, PaaS, SaaS 클라우드 키 관리

- CipherTrust 클라우드 키 관리자로 Microsoft Azure Key Vault, Microsoft Office 365, Salesforce Shield Platform Encryption, Amazon Web Services Key Management Services 간의 상호 운용성을 활용해 암호키를 제어하고 관리할 수 있습니다.

❖ KMIP 클라이언트용 키 관리

- Cisco, Nutanix, NetApp, Dell Technologies, MongoDB 등, KMIP(Key Management Interoperability Protocol) 호환 암호화 솔루션의 키를 관리합니다.

❖ TDE 키 관리

- Oracle, Microsoft, IBM의 TDE(투명한 데이터 암호화)용 암호키를 관리하고 안전하게 저장합니다.

I 하드웨어 보안모듈 HSM 레퍼런스

- 지자체 · 공공 · 기업 · 금융 · 민수 등 1100여개 고객사 레퍼런스 보유

금융

I 제품 견적 및 문의

- 제 조 사 : (주)비센스바움
- 홈페이지 : wissensbaum.com
- 연락처 : Tel 070-4350-1491 / Fax 02-557-9875
- 담당자 : 오주철 / cs@wissensbaum.com / 010-8743-9650
- 서주원 / jwseo@wissensbaum.com / 010-9159-8229



