



ENTRUST



Qube Cinema는 Entrust nShield HSM의 도움으로 디지털 시네마 배포에 혁명을 일으켰습니다

KeySmith

QUBE

디지털 시네마 기술 제조업체가 신뢰할 수 있는 최고 수준의 콘텐츠 보호를 제공하여 디지털 시네마 배포용 온라인 키 관리 시장을 주도한 방법.

디지털 시네마 용 서버, 프로젝터, 마스터링 및 배포 기술 제조업체인 Qube Cinema는 영화 산업이 물리적 배포에서 디지털 배포로 10년 동안의 전환을 완료하면서 매우 파괴적인 기술을 시장에 도입할 수 있는 독특한 기회를 찾았습니다. 디지털은 엄청난 이점을 제공했습니다. 하드 드라이브를 제작하고 전송하는 것이 여러 필름 인쇄 릴보다 훨씬 저렴했습니다. 디지털 필름은 훨씬 더 빨리 배포되어 유통 업체가 수요를 더 잘 충족할 수 있습니다. 디지털 영화는 시간이 지나도 품질이 저하되지 않으며 숙련되지 않은 노동력으로도 상영할 수 있습니다.

아날로그에서 디지털로 전환하는 데 있어 영화 산업이 다른 산업에 뒤쳐진 가장 큰 장애물은 보안이었습니다. 콘텐츠 소유자(영화 제작사)는 불법 복제에 대해 엄청나게 우려했고 매우 강도 높은 보안 조치를 원했습니다. 반면에 극장 소유주와 배급사는 수익성에 해를 끼치고 운영 부담을 유발하는 복잡하거나 값비싼 보안 조치를 처리할 필요가 없었습니다. Qube 팀은 작동하기 매우 쉬운 최고 등급의 보안으로 디지털 시네마 키를 온라인으로 관리하는 효율적인 방법을 찾을 수 있다면 업계에 혁명을 일으킬 수 있다는 것을 깨달았습니다.



솔루션: KEYSMITH: POWERED ENTRUST NSHIELD HSM으로 구동되는 온라인 키 관리 시스템

디지털 시네마 배포시 효율적인 보안에 대한 요구를 해결하기 위해 Qube는 Entrust nShield® HSM(하드웨어 보안 모듈)을 사용하여 업계에서 가장 강력한 보안 수준을 갖춘 사용하기 쉬운 배포 시스템을 개발했습니다. 디지털 시네마에서 영화는 디지털 시네마 패키지(DCP)로 인코딩 및 암호화되고 하드 드라이브 또는 위성 피드를 통해 배포된 다음, 영화의 특정 극장, 기간 및 상영 횟수에 대한 잠금을 해제하는 고유한 KDM(키 전달 메시지)에 포함된 정보를 사용하여 극장에서 해독할 수 있습니다.

KeySmith는 콘텐츠 소유자와 배포자의 요구 사항을 모두 충족합니다. 콘텐츠 소유자는 더 이상 배포자가 일반적으로 사용하는 소프트웨어 기반의 사내 암호화 조치 또는 최악의 시나리오(암호화 키 분실 및 자체 콘텐츠 잠금)에 대해 걱정할 필요가 없게 됩니다. Entrust nShield HSM은 업계에서 콘텐츠 암호화 키에 대해 최고 수준의 보호를 제공하는 동시에 키가 손실되지 않도록 보호합니다. 배급사 및 극장 소유주에게 Qube 시스템은 높은 보안 구현에 대한 장벽이나 여러 편의 때문에 보안을 희생하고 싶은 유혹을 없애줄 정도로 운영이 쉽습니다.

시스템 작동 방식은 다음과 같습니다. 스튜디오 또는 독립 영화 제작자가 배포를 위해 영화를 제출합니다. 이것을 영화를 구성하는 미디어 파일 및 메타 데이터에 대한 업계 표준 형식인 DCP로 변환합니다. DCP 내에서 AES 키 세트는 개별 파일을 암호화하는 데 사용됩니다. 이러한 키를

안전하게 전달하는 배포 KDM(DKDM)은 배포자의 KeySmith 계정에 제공됩니다. 이 DKDM을 통해 KeySmith는 개별 극장에 대한 KDM을 생성할 수 있습니다. Entrust nShield HSM은 KeySmith 내의 각 회사에 대해 고유한 RSA 공개/개인 키 쌍 및 관련 디지털 인증서를 생성합니다. 이러한 HSM은 HSM의 인증된 보안 경계 내에서 실행되는 애플리케이션을 사용하여 수신 극장의 공개 키와 함께 AES 키를 암호화합니다. 의도한 수신자만 제조시 보유하고 안전하게 설치된 관련 개인 키를 사용하여 패키지를 해독할 수 있습니다. KeySmith는 KDM을 극장에 직접 전달할 수도 있습니다. 이것은 일반적으로 극장이 하드 드라이브 또는 위성 다운로드를 통해 영화를 수신한 후에 수행됩니다. 배급사에게 사용 편의성을 제공하는 동시에 Qube 비즈니스 가치 제안의 두 가지 중요한 요소인 영화 콘텐츠의 높은 보증 보호를 보장하는 매우 효율적인 시스템입니다.

솔루션 정보

Entrust nShield HSM은 암호화 처리, 키 보안 및 관리를 안전하게 이행할 수 있도록 강화된 조작 방지 환경을 제공합니다. 이 제품으로는 암호 시스템과 모범 사례에 관련하여 널리 인정받는 표준과 새로운 표준 모두를 충족하고, 고도로 정밀한 보안 솔루션을 배포할 수 있을 뿐만 아니라 고도로 효율적인 운영 수준을 유지할 수 있습니다.

Entrust nShield HSM은 독립 기관의 인증을 받았으며, 정량화가 가능한 보안 벤치 마크를 설정하여 규정 준수 의무 및 내부 정책을 지원할



수 있다는 확신을 고객에게 제공합니다. Entrust nShield HSM은 휴대용 장치에서 고성능 데이터 센터 어플라이언스에 이르는 모든 일반적인 배포 시나리오를 지원하기 위해 다양한 폼 팩터로 제공됩니다.

Entrust nShield HSM을 사용하면 다음과 같은 장점을 누릴 수 있습니다.

- 변조 방지 하드웨어 내에서 암호키 및 암호화 작업에 인증 받은 보안을 제공하여 중요한 애플리케이션에 한층 강화된 안전성 제공
 - 암호화를 비용 효율적으로 가속화하고, 기존 데이터센터나 클라우드 환경과는 비교할 수 없는 운영 유연성 확보
 - 소프트웨어 한정 암호화의 보안 취약성과 성능 문제 극복
 - 규제 준수 관련 비용 절감, 백업 및 원격 관리 등을 비롯한 일상적인 키 관리 업무 축소
- Entrust nShield HSM을 사용하면 필요한 용량만 구매하고 요구 사항 변화에 맞추어 손쉽게 솔루션을 확장할 수 있습니다

ENTRUST NSHIELD CODESAFE

CodeSafe 개발자 툴킷은 민감한 애플리케이션을 nShield HSM의 보호 경계 내에서 이동할 수 있는 고유한 기능을 제공합니다. FIPS 140-2 Level 3 HSM에서 안전하게 로딩하고 실행함으로써, 애플리케이션을 조작으로부터 보호하고 보안 환경 내에서 데이터를 해독, 처리 및 암호화할 수 있습니다.

CodeSafe는 다음과 같은 장점을 제공합니다.

- 환경에 관계없이 민감한 애플리케이션에 대한 원격 제어를 제공하고, 고객이 사용하는 운영체제

또는 구성에 관계없이 서버나 메인프레임을 가리지 않고 암호화 서비스를 제공하여 지적 재산 도난을 방지합니다. 또한 CodeSafe를 사용하면 애플리케이션 소유자가 물리적으로 다른 위치에서도 최신 애플리케이션 실행 환경을 유지할 수 있습니다.

- **출시 전에 무결성을 확인할 수 있도록** 신뢰할 수 있는 애플리케이션에 디지털 서명 기능을 제공하여 해커나 불량 관리자의 공격으로부터 애플리케이션을 보호합니다. 또한 CodeSafe는 아웃소싱 및 계약을 활용하는 통제되지 않은 환경에서도 애플리케이션을 도난으로부터 보호합니다.
- **진정한 종단간 SSL** 암호화를 제공하고, SSL을 종료하며, HSM 내에서 민감한 데이터를 처리하여 공격으로부터 보호함으로써 민감한 SSL 데이터를 보호합니다.

왜 ENTRUST일까요?

Entrust를 사용하기로 한 Qube의 결정에 영향을 준 주요 요인은 다음과 같습니다.

- **CodeSafe.** Entrust nShield HSM은 다른 솔루션이 제공하지 않는 보안 기능을 제공합니다. 즉 CodeSafe를 사용하면 표준 서버 기반 플랫폼에 만연하는 공격으로부터 보호되는 안전한 환경(HSM 내부)에서 애플리케이션을 실행할 수 있습니다. Qube는 CodeSafe를 사용하여 모든 키 처리 및 암호화/복호화 작업을 수행하여 가능한 최고 수준의 보안을 제공했습니다.
- **신뢰성과 명성.** Qube는 스튜디오와 영화 산업의 신뢰를 얻으려면 최고 수준의 검토를 견딜 수 있는 가장 안정적이고 신뢰할 수 있는 보안 솔루션을 선택해야 한다는 것을 알고 있었습니다.



주요 이점

- 신뢰할 수 있는 환경 내에서 실행하여 호스트 측 애플리케이션의 보안 취약성을 극복
- 조작, 맬웨어 및 트로이 목마로부터 중요한 애플리케이션을 보호
- 다양한 연결 장치를 지원하기 위해 HSM 암호화 서비스 제공
- FIPS 140-2 Level 3 승인 변조 방지 하드웨어로 인증된 보호 제공
- 키 관리 작업 비용 절감

검증된 성능, 변조 방지 하드웨어 및 암호키에 대한 FIPS 140-2 Level 3 인증 보호 기능을 갖춘 Entrust nShield HSM은 이 요구 사항에 완벽하게 부합합니다.

- **탄력성 및 가용성.** Entrust nShield HSM을 통해 Qube는 유통 업체에 키 가용성을 보장할 수 있습니다. 이는 이러한 서비스 산업에서 신뢰를 키우는 데 중요한 측면입니다. Qube는 복원력을 보장하기 위해 여러 지리적 위치에서 실행되는 Entrust nShield HSM을 통해 키를 쉽게 백업하고 여러 HSM을 동기화 상태로 유지하여 글로벌 사용자에게 키를 제공할 수 있습니다.

- **확장성.** Entrust nShield HSM을 사용하면 Qube가 디지털 시네마 제공업체에 제공하는 키(온라인 서비스의 잠재적 성장에 중요한)를 무제한으로 발급하고 관리할 수 있습니다.
- **대응성.** Qube는 Entrust에서 받은 사전 및 사후 판매 서비스와 지원 수준에 깊은 인상을 받았습니다.

ENTRUST 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. 2,500명이 넘는 동료 및 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