



ENTRUST



Qube Cinema ha rivoluzionato la distribuzione nel cinema digitale con l'aiuto degli HSM nShield di Entrust

KeySmith

QUBE

Il produttore di tecnologia domina il mercato della gestione delle chiavi online per la distribuzione digitale, offrendo livelli superiori di protezione dei contenuti.

Iniziato oltre 10 anni fa, il passaggio dalla distribuzione fisica a quella digitale dei contenuti cinematografici si è rivelato un processo tutt'altro che rapido ed è proprio in questo contesto che Qube Cinema, azienda produttrice di server, proiettori, tecnologie di masterizzazione e distribuzione per il cinema digitale, ha intravisto un'opportunità unica di introdurre sul mercato una tecnologia rivoluzionaria. I vantaggi del digitale sono enormi: prima di tutto, è molto meno costoso produrre e inviare un unico disco rigido per ogni film rispetto a varie bobine di pellicola. I tempi di distribuzione dei contenuti in formato digitale, poi, risultano ridotti, consentendo ai distributori di soddisfare meglio la domanda. Infine, le copie digitali non si deteriorano nel tempo e possono essere proiettate da operatori meno qualificati.

Il più grande ostacolo, però, è sempre stato rappresentato dalla sicurezza, che è anche il motivo per cui questa transizione è stata più lenta per l'industria cinematografica rispetto ad altri settori. Preoccupati dalla pirateria, i proprietari dei contenuti, ovvero le aziende di produzione cinematografica, richiedevano misure di protezione straordinariamente elevate. Al tempo stesso, i proprietari delle sale e i distributori non volevano dover fare i conti con misure di sicurezza complicate o costose, che avrebbero danneggiato la redditività e introdotto oneri operativi. Per questo, il team di Qube sapeva che, per rivoluzionare il settore, avrebbe dovuto sviluppare un sistema efficiente di gestione delle chiavi per il cinema digitale online, caratterizzato da una sicurezza superiore e da una grande facilità d'uso.

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

LA SOLUZIONE: KEYSMITH, UN SISTEMA DI GESTIONE DELLE CHIAVI ONLINE SUPPORTATO DAGLI HSM NSHIELD DI ENTRUST

Per rispondere alle esigenze di sicurezza ed efficienza nella distribuzione di contenuti in formato digitale, Qube ha implementato gli hardware security module (HSM) nShield® di Entrust, sviluppando un sistema facile da usare e caratterizzato dal più alto livello di sicurezza disponibile nel settore. Nel cinema digitale, i film vengono codificati e cifrati in un pacchetto chiamato "Digital Cinema Package" (DCP), distribuito tramite disco rigido o feed satellitare. Una volta in sala, il pacchetto viene decifrato con le informazioni contenute in un Key Delivery Message (KDM) univoco, che sblocca il film per un determinato cinema, periodo di tempo e numero di proiezioni.

KeySmith soddisfa le esigenze tanto dei proprietari di contenuti quanto dei distributori. I proprietari, infatti, non devono più preoccuparsi delle misure crittografiche basate su software, spesso insufficienti, adottate dai distributori né della potenziale perdita delle chiavi di crittografia, una situazione tanto estrema quanto catastrofica che potrebbe portarli a non accedere più ai propri contenuti. Gli HSM nShield di Entrust offrono una protezione ineguagliata delle chiavi usate per crittografare i contenuti, garantendo al contempo che queste non vadano mai perse. Per i distributori e i proprietari delle sale, il sistema di Qube offre anche un buon livello di semplicità operativa, un fattore determinante per eliminare eventuali ostacoli all'implementazione di una soluzione sicura o per allontanare la tentazione di sacrificare la sicurezza in nome della praticità.

Ma come funziona il sistema? Prima di tutto, uno studio o un regista indipendente presenta un film per la distribuzione. Questo viene convertito in un DCP, un formato standard di settore per i file multimediali e i metadati di un contenuto cinematografico.

Al suo interno, i singoli file vengono cifrati con un set di chiavi AES protette in un Distribution Key Delivery Message (DKDM) che, reso disponibile sull'account KeySmith del distributore, permette al sistema di generare i KDM per le singole sale. Gli HSM nShield di Entrust creano una coppia univoca di chiavi pubbliche/private RSA e il certificato digitale associato per ogni azienda all'interno di KeySmith. Cifrano inoltre le chiavi AES con la chiave pubblica della sala destinataria, utilizzando un'applicazione in esecuzione all'interno del proprio margine di sicurezza hardware certificato. L'effettivo destinatario è il solo a poter decifrare il pacchetto con la relativa chiave privata, che è univoca e viene installata in modo sicuro durante la produzione. KeySmith può anche distribuire i KDM direttamente alle sale cinematografiche, ma questo, di solito, avviene dopo che il film è stato ricevuto tramite disco rigido o download satellitare. Efficiente e facile da usare per i distributori, il sistema garantisce inoltre una protezione a elevata garanzia dei contenuti, tre attributi strategici della proposta di valore di Qube.

DETTAGLI DELLA SOLUZIONE

Gli HSM nShield di Entrust forniscono un ambiente affidabile a prova di manomissione per offrire attività sicure di elaborazione crittografica, protezione e gestione delle chiavi. Consentono inoltre di implementare soluzioni a elevata sicurezza, che soddisfano standard di diligenza consolidati ed emergenti per i sistemi e i processi crittografici, mantenendo comunque alti i livelli di efficienza operativa.

Gli HSM nShield di Entrust sono certificati da autorità indipendenti, che stabiliscono benchmark di sicurezza quantificabili per assicurare che i clienti rispettino gli obblighi di conformità e le norme aziendali. Sono inoltre disponibili in vari fattori di forma adatti agli scenari di implementazione più comuni, dai dispositivi portatili alle appliance ad alte prestazioni nei data center.

Con gli HSM nShield di Entrust è possibile:

- Ottimizzare la sicurezza delle applicazioni critiche fornendo una protezione certificata per le chiavi e le operazioni crittografiche all'interno di hardware a prova di manomissione.
- Ottenere un'accelerazione crittografica a costi contenuti e una flessibilità operativa ineguagliata tanto nei data center tradizionali quanto negli ambienti cloud.
- Superare i rischi di sicurezza e le difficoltà prestazionali della crittografia basata unicamente su software.
- Ridurre i costi per il raggiungimento della conformità normativa e lo svolgimento delle attività quotidiane relative alle chiavi, tra cui il back-up e la gestione remota. Gli HSM nShield di Entrust consentono alle aziende di acquistare solo la capacità di cui hanno bisogno, ma offrono la scalabilità necessaria a ridimensionare la soluzione in risposta all'evoluzione delle esigenze.

NSHIELD CODESAFE DI ENTRUST

Il kit di strumenti per sviluppatori nShield CodeSafe offre l'esclusiva possibilità di trasferire le applicazioni sensibili all'interno del perimetro protetto di un HSM nShield certificato. Caricate ed eseguite in totale sicurezza all'interno di HSM conformi allo standard FIPS 140-2 di livello 3, le applicazioni risultano protette dalla manipolazione e possono decifrare, elaborare e cifrare nuovamente i dati all'interno di un ambiente sicuro.

CodeSafe consente alle organizzazioni di:

- Prevenire il furto della proprietà intellettuale, garantendo il controllo remoto delle applicazioni sensibili in qualsiasi ambiente e offrendo servizi

di crittografia compatibili con tutti i sistemi operativi e le configurazioni adottati dai clienti, che si tratti di server o mainframe. Permette inoltre ai proprietari di applicazioni e dispositivi portatili di mantenere aggiornato l'ambiente di esecuzione da remoto.

- **Proteggere le applicazioni dagli attacchi** di hacker o amministratori disonesti, dando la possibilità di firmare digitalmente quelle affidabili per verificarne l'integrità prima del lancio. In più, salvaguarda le applicazioni dal furto, anche in ambienti non controllati, come nel caso di esternalizzazione e appalti.
- Affidarsi alla crittografia SSL end-to-end, terminare le sessioni SSL ed **elaborare i dati sensibili all'interno dell'HSM per proteggerli** dagli attacchi.

PERCHÉ ENTRUST?

La decisione di Qube di implementare i prodotti di Entrust è stata influenzata da diversi fattori:

- **CodeSafe:** funzionalità di sicurezza unica degli HSM nShield di Entrust, CodeSafe consente l'esecuzione delle applicazioni all'interno dell'HSM, un ambiente sicuro dove vengono protette dagli attacchi frequenti nelle piattaforme standard basate su server. Qube utilizza CodeSafe per eseguire tutte le operazioni di gestione delle chiavi e di cifratura/decriptazione, garantendo una sicurezza di massimo livello.
- **Affidabilità e reputazione:** Qube sapeva che, per ottenere la fiducia non solo degli studi cinematografici ma dell'intero settore, avrebbe dovuto selezionare le soluzioni di sicurezza più affidabili e credibili, che avrebbero soddisfatto anche i requisiti più rigorosi.

VANTAGGI PRINCIPALI

- **Superamento dei rischi di sicurezza** legati alle applicazioni lato host eseguendole all'interno di un ambiente affidabile
- **Tutela delle applicazioni critiche** da manipolazioni, malware e trojan
- **Implementazione di servizi di crittografia basati su HSM** per supportare un'ampia gamma di dispositivi connessi
- **Protezione certificata con hardware** approvato a prova di manomissione, conforme allo standard FIPS 140-2 di livello 3
- **Riduzione dei costi relativi alle attività di gestione delle chiavi**

Grazie a prestazioni comprovate, hardware a prova di manomissione e una protezione certificata secondo lo standard FIPS 140-2 di livello 3 per le chiavi crittografiche, gli HSM nShield di Entrust si sono rivelati la scelta ideale sotto ogni aspetto.

- **Resilienza e disponibilità:** gli HSM nShield di Entrust permettono a Qube di garantire la disponibilità delle chiavi ai distributori, un aspetto essenziale per stabilire un rapporto di fiducia in questo settore. Grazie all'esecuzione degli HSM nShield di Entrust in più aree geografiche per garantire la resilienza del sistema, Qube può eseguire il back-up delle chiavi e mantenere più HSM sincronizzati per distribuire le chiavi a utenti di tutto il mondo.

- **Scalabilità:** gli HSM nShield di Entrust permettono a Qube di emettere e gestire un numero illimitato di chiavi, un requisito fondamentale per rimanere al passo con la potenziale crescita futura del servizio online che l'azienda offre ai fornitori di cinema digitale.
- **Reattività:** Qube è rimasta molto colpita dal livello di assistenza e supporto pre- e post-vendita ricevuto da Entrust.

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.