



ENTRUST



Prima Cinema desarrolla un nuevo mercado para películas de estreno utilizando HSMs nShield de Entrust

P R I M ATM
C I N E M A

Cómo una compañía de medios de comunicación a supera los problemas de seguridad del estudio para llevar películas recién estrenadas directo a los cines en casa.

EL DESAFÍO: DESARROLLAR UNA MANERA SEGURA PARA ENTREGAR PELÍCULAS RECIÉN LANZADAS DIRECTAMENTE A UN PÚBLICO DOMÉSTICO

Los fundadores de PRIMA Cinema querían aprovechar una nueva oportunidad de mercado para ofrecer películas recién estrenadas a clientes con sistemas de cine en casa, al mismo tiempo que las películas se exhibían en los cines. La cantidad de sistemas de cine en casa de alta gama que se construían cada año crecía rápidamente, ya que la cantidad de personas interesadas en ver películas desde casa en lugar de en el cine aumentaba constantemente. El equipo de PRIMA Cinema sintió que podía hacer una obra importante al llevar películas con calidad de teatro a los cines en casa, si pudieran resolver el mayor obstáculo: la seguridad.

La piratería de películas es una gran preocupación para los estudios y distribuidoras que, de acuerdo a algunas, pierden miles de millones de dólares cada año cuando las propiedades de películas y televisión se copian y distribuyen ilegalmente. Cuando las películas se exhiben en los cines, los directores de los cines pueden monitorear al público para evitar la “cámara” (grabar películas en el cine con una cámara de video), pero para los cines en casa, se necesitaría un tipo de seguridad diferente. El equipo de PRIMA sabía que para conseguir la aceptación de los estudios y de otros propietarios de contenido para su modelo de negocio, tendrían que idear una forma muy segura de distribuir y mostrar películas, sin disminuir la experiencia del espectador.

APRENDA MÁS EN [ENTRUST.COM/HSM](https://entrust.com/hsm)



LA SOLUCIÓN: MÚLTIPLES CAPAS CRIPTOGRÁFICAS UTILIZANDO HSMs nSHIELD DE ENTRUST

Para abordar las preocupaciones de los estudios y distribuidores, PRIMA Cinema desarrolló un sistema para codificar y distribuir películas a los cines en casa que involucraba múltiples capas de cifrado, así como una autenticación sólida entre sus servidores y dispositivos de reproducción domésticos, utilizando módulos de seguridad de hardware (HSMs) nShield® de Entrust para generar y proteger claves privadas de cifrado y firma digital.

Antes de la distribución, PRIMA Cinema cifra las películas utilizando AES de 256 bits con claves generadas por un HSM. El dispositivo de reproducción instalado en los cines domésticos incluye un módulo de plataforma confiable (TPM) donde se protegen y gestionan las claves privadas y los certificados asociados con el descifrado y la autenticación del dispositivo.

Durante la fabricación, las claves nunca se exponen fuera del HSM y del dispositivo consumidor: la aplicación que controla todo el procesamiento criptográfico y el manejo de claves se ejecuta dentro de los límites seguros del HSM utilizando la capacidad única de nShield CodeSafe. Las funciones de acceso basado en roles de nShield Security World, comunes a todos los HSMs nShield, garantizan que se apliquen los controles administrativos de varias personas para ayudar a prevenir la posibilidad de un ataque interno al sistema. Las películas se transfieren a los dispositivos de reproducción a través de banda ancha y están protegidas con autenticación bidireccional basada en certificados. Además, un lector biométrico de huellas dactilares integrado en el dispositivo de reproducción garantiza que solo los verdaderos propietarios registrados puedan iniciar una evaluación. Finalmente, en el momento de la reproducción, el HSM genera una marca de agua específica de la sesión y se usa para marcar el video de manera invisible para disuadir la grabación de la película.

El enfoque de seguridad de PRIMA Cinema fue sometido a una revisión independiente y se encontró que satisfacía los requisitos altamente estrictos de los proveedores de contenido, y le permitió a la compañía proceder al mercado como la primera compañía en la historia del cine en obtener derechos de licencia y distribución de películas estrenadas en cines para la privacidad de los cines en casa.

ACERCA DE LA SOLUCIÓN

Los HSMs nShield de Entrust proporcionan un entorno reforzado y resistente a manipulaciones indebidas para realizar un procesamiento criptográfico seguro, la protección y administración de claves. Con estos dispositivos puede implementar soluciones de alta seguridad que cumplen con los estándares establecidos y emergentes de cuidado debido para los sistemas criptográficos y las prácticas recomendadas, mientras que también mantiene altos niveles de eficiencia operacional.

Los HSMs nShield de Entrust están certificados por autoridades independientes, lo que establece puntos de referencia de seguridad cuantificables que le brindan confianza en su capacidad para respaldar los mandatos de cumplimiento y las políticas internas. Los HSMs nShield de Entrust están disponibles en varios factores de forma para admitir todos los escenarios de implementación comunes, desde dispositivos portátiles hasta dispositivos de centro de datos de alto rendimiento.

Con los HSMs nShield de Entrust usted puede:

- Ofrecer protección certificada para claves criptográficas y operaciones en un hardware a prueba de manipulaciones indebidas para mejorar la seguridad para aplicaciones críticas
- Logre entornos de nube y aceleración criptográfica rentables
- Superar las vulnerabilidades de seguridad y los retos de rendimiento de la criptografía de software



- Reducir el coste de cumplimiento con la normativa y las tareas cotidianas de gestión de claves que incluyen las copias de seguridad y la gestión remota. Con los HSMs nShield de Entrust, puede comprar la capacidad que necesite y escalar su solución de forma fácil y a medida que sus necesidades cambien.

NSHIELD CODESAFE

El kit de herramientas para desarrolladores nShield CodeSafe proporciona la capacidad única para mover aplicaciones confidenciales dentro del perímetro protegido de un HSM nShield certificado FIPS 140-2 Nivel 3. Con este enfoque, las aplicaciones están protegidas de las manipulaciones indebidas y pueden descifrar, procesar y cifrar datos dentro del entorno seguro.

nShield CodeSafe permite que las organizaciones:

- Prevenir el robo de propiedad intelectual proporcionando control remoto de aplicaciones confidenciales sin importar el entorno, y ofreciendo servicios criptográficos independientemente del sistema operativo o la configuración utilizada por el cliente, ya sea servidor o computador central. nShield CodeSafe también les permite a los propietarios de aplicaciones o dispositivos portátiles mantener un entorno de ejecución de aplicaciones actualizado sin presencia física.
- Proteger las aplicaciones de ataques por parte de hackers o administradores deshonestos al brindar la capacidad de firmar digitalmente aplicaciones confiables para que se verifique su integridad antes de su lanzamiento. nShield CodeSafe también protege las aplicaciones contra el robo, incluso en entornos no controlados que utilizan la subcontratación y la contratación.
- Proteger los datos confidenciales de SSL proporcionando un verdadero cifrado SSL de extremo a extremo, SSL de terminación y procesamiento los datos confidenciales dentro del HSM para protegerlos de los ataques.

¿POR QUÉ ENTRUST?

Entrust ganó el negocio basándose en la seguridad y funcionalidad de sus HSMs nShield que proporcionaban:

- **Mayor seguridad.** Desde el principio, el equipo de PRIMA Cinema sabía que para obtener la aprobación de los estudios necesitaría la seguridad de mayor garantía de un enfoque de dispositivo reforzado y certificado por FIPS en lugar de utilizar plataformas de aplicación estándar intrínsecamente más riesgosas. Y PRIMA Cinema necesitaba una solución comprobada con certificaciones de seguridad para que cualquiera que revisara el sistema quedara satisfecho en cuanto a su confiabilidad y pedigrí de seguridad. Y querían un enfoque de seguridad de varias capas, utilizando algoritmos estándar de la industria y longitudes de clave adecuadas para la protección más sólida disponible. HSMs nShield de Entrust entregados para todas las cuentas:
- **nShield CodeSafe.** Los HSMs nShield de Entrust proporcionan una función de seguridad que ninguna otra solución ofrece. CodeSafe permite que las aplicaciones se ejecuten en un entorno seguro, dentro del HSM, donde se hallan protegidas de los ataques que prevalecen en las plataformas estándar basadas en servidores. PRIMA Cinema utilizó CodeSafe para realizar todas las operaciones de manejo de claves y cifrado/descifrado, proporcionando el mayor nivel de seguridad posible.



VENTAJAS PRINCIPALES

- Superar las vulnerabilidades de realizar funciones de seguridad en plataformas de aplicaciones estándar, ejecutándolas en su lugar dentro de un entorno confiable
- Proteger las aplicaciones críticas y las claves secretas de cifrado y firma de la manipulación indebida, el malware y los troyanos
- Poner a disposición los servicios criptográficos del HSM para admitir una amplia variedad de dispositivos de conexión
- Ofrecer protección certificada con hardware resistente a manipulaciones aprobado por FIPS 140-2 Nivel 3
- Reducir el costo de las tareas de gestión de claves

• **Arquitectura nShield Security World.**

La arquitectura de nShield Security World optimizó la gestión de claves y permitió a PRIMA construir y administrar su sistema general al facilitar la definición de toda la seguridad estricta y el control requerido por el proyecto. La arquitectura Security World proporciona una experiencia unificada de administrador y usuario y garantiza la interoperabilidad tanto si se implementan uno como cientos de dispositivos.

- **Experiencia de usuario superior.** Los HSMs nShield de Entrust pudieron brindar de manera transparente la sólida seguridad requerida por los estudios sin interferir o comprometer la calidad de la experiencia del usuario, una necesidad absoluta para la propuesta de valor de PRIMA Cinema.

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.



Aprenda más en
entrust.com/HSM



ENTRUST