Traiga su propia llave (BYOK) de nShield les permite a los clientes de la nube obtener un mayor control sobre la seguridad de los datos

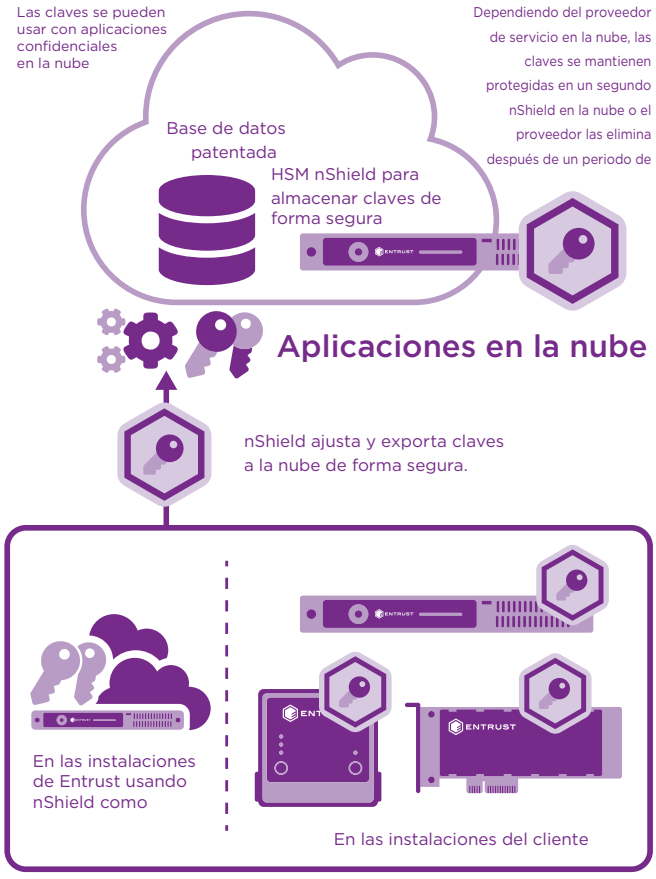
La comodidad de la nube satisface la seguridad

CARACTERÍSTICAS PRINCIPALES

- Prácticas de administración de claves más seguras que fortalecen la seguridad de sus datos confidenciales en la nube.
- Generación de claves más sólida usando el generador de número aleatorio de alta entropía Entrust de nShield®, que está protegido con hardware con certificación FIPS
- Mayor control sobre sus claves, utilice sus propios HSMs nShield en su propio entorno para crear, exportar y almacenar de forma segura sus claves en la nube
- Operaciones de administración de claves más uniformes, independientemente de si sus claves se usan en la nube o de forma local

Con los HSMs nShield, usted puede traer sus propias llaves (BYOK) a sus aplicaciones en la nube, ya sea que esté utilizando los servicios web de Amazon (AWS), Google Cloud Platform (GCP) o Microsoft Azure.

Los HSMs nShield de gran confianza, le permiten seguir beneficiándose de la flexibilidad y la economía de los servicios en la nube, al tiempo que refuerza la seguridad de sus prácticas de administración de claves y obtiene mayor control sobre sus claves.



La arquitectura única de Entrust, Security World, ofrece almacenamiento seguro a largo plazo y la protección para recuperación en caso de desastres de las claves maestras.

APRENDA MÁS EN ENTRUST.COM/HSM

Traiga su propia llave (BYOK) de nShield

Qué hace BYOK de nShield

Con BYOK de nShield podrá usar sus HSMs de nShield para generar, almacenar y administrar las claves con las que protege sus aplicaciones confidenciales hospedadas en la nube, bases de datos y almacenamiento masivo. BYOK de nShield ofrece estas funcionalidades:

- Confíe en la raíz de confianza del hardware. Sus HSMs nShield son dispositivos altamente fiables a prueba de manipulaciones, con certificación FIPS 140-2 Nivel 3. Estos HSMs sirven de raíz de confianza para sus servicios en la nube, permitiéndole generar y proteger su cifrado y claves de firma de forma segura.
- Use nShield para administrar sus claves. Cuando tiene datos confidenciales almacenados en sus aplicaciones hospedadas den la nube, puede confiar en sus HSMs nShield para generar y ajustar sus claves, y enviarlas de forma segura a sus aplicaciones en la nube.
- Controle la disponibilidad de sus claves. Puesto que usted exclusivamente controla su HSM nShield, independientemente de forma local o en nShield como entorno del servicio, usted decide cuándo se generan o exportan las claves. Al controlar la clave maestra, también controla cuándo y si se realizan más exportaciones a su proveedor de nube.
- Elija su proveedor de nube. Con BYOK de nShield, usted decide qué proveedor de nube usar para cada clave. Esto le da la flexibilidad de elegir la nube correcta, ya sea desde su nShield local o como entorno del servicio para sus diferentes aplicaciones, mientras se beneficia de la generación y protección de claves de alta seguridad de nShield.

Primeros pasos con BYOK de nShield

Para empezar a usar BYOK de nShield para AWS, GCP o Azure, necesitará un HSM nShield. Puede elegir entre las siguientes soluciones:

- nShield Connect, un dispositivo conectado a la red.
- nShield Solo, una tarjeta PCIe integrada en el servidor.
- nShield Edge, un dispositivo conectado por USB para aplicaciones de bajo volumen.
- nShield como servicio, usando HSMs nShield Connect por suscripción

Para obtener la máxima seguridad con Microsoft Azure, elija Entrust BYOK. Ver: **docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-Entrust Si necesita ayuda con la implementación, el siguiente paquete opcional está disponible para su compra:**

Traiga su propia llave, servicios profesionales de Azure
Este paquete incluye un nShield Edge, integración por parte del equipo de servicios profesionales de Entrust y un año de mantenimiento.

También puede comprar HSMs nShield Connect, Solo, o Edge y los servicios profesionales de forma independiente.

Para usar nShield BYOK con AWS, GCP o Microsoft Azure utilizando el método de estándares abiertos de Microsoft, necesitará el siguiente paquete de Entrust:

Paquete opcional de integración en la nube
Este paquete opcional contiene todo lo que necesita para usar sus HSMs nShield de forma local para generar empaquetamiento, transportar de forma segura y arrendar sus claves a AWS o GCP o Microsoft Azure mediante Azure BYOK.

Puede integrar nShield BYOK con AWS GCP o Azure usted mismo, o puede usar los servicios profesionales de Entrust para que le ayuden a hacer la conexión de forma eficiente.

Traiga su propia llave (BYOK) de nShield

Cómo funciona BYOK de nShield

Entrust ofrece los mecanismos que le permiten usar sus HSMs nShield para generar claves, proteger el almacenamiento a largo plazo y exportar sus claves a la nube. Cuando sus claves se hayan exportado a la nube desde su nShield local o como un servicio, podrá administrar las claves de acuerdo con uno de los siguientes enfoques:

Si usa Microsoft Azure:

Para obtener la máxima seguridad con Microsoft Azure, elija Entrust BYOK. Esto controla las condiciones que deben cumplirse para permitir que una clave se cargue en Azure y restringe estrictamente lo que MSFT puede hacer con ella una vez que está allí.

Transferirá sus claves al HSM nShield de forma segura desde la infraestructura Azure para obtener la seguridad del HSM en ambos extremos.

Si usa AWS o GCP:

Asignará sus claves a AWS o GCP para un uso temporal en la nube. Después de un periodo predeterminado, sus claves en la nube se destruirán. Si es necesario, puede volver a asignar las claves almacenadas en su HSM.

Sea cual sea el servicio en la nube pública que elija, generar sus propias claves y controlar su exportación le ayuda a establecer salvoconductos sólidos para datos confidenciales y aplicaciones en la nube.

HSMs de Entrust

Los HSMs nShield de Entrust se encuentran entre las soluciones de HSMs de mayor rendimiento, las más seguras y fáciles de integrar que se encuentran disponibles, lo cual facilita el cumplimiento normativo y ofrece los niveles más altos de seguridad de datos y aplicaciones para organizaciones empresariales, financieras y gubernamentales. Nuestra exclusiva arquitectura de administración de claves Security World proporciona controles sólidos y granulares sobre el acceso y uso de claves.

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Para saber más sobre los HSMs nShield de Entrust

HSMinfo@entrust.com

entrust.com/HSM

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

Contáctenos:
HSMinfo@entrust.com