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

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 confidentinzli: 10 6.322 -10.69T 4.5 (d)-10.4 (e)-12.1 (n l)-3.4 (a n)-21 (u

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**