THALES

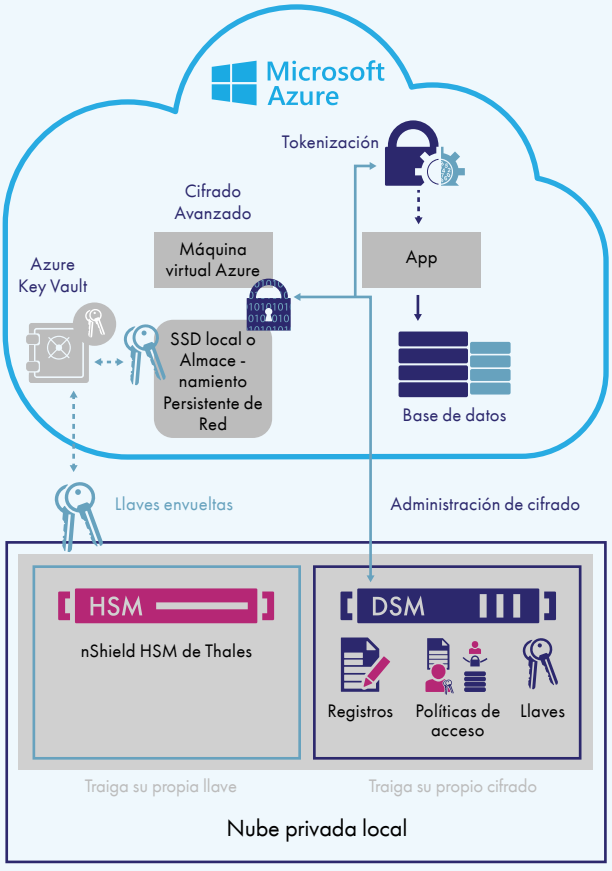
www.thalesesecurity.com

CIFRADO AVANZADO CON ADMINISTRACIÓN COMPLETA DE LLAVES

- Evite el bloqueo de cifrado del proveedor y asegure la movilidad de datos que necesita mientras distribuye las cargas de trabajo y los datos de manera eficiente y segura a través de varios proveedores de la nube, incluidos Microsoft Azure, con administración de cifrado centralizado e independiente
- Aproveche en forma segura las ventajas del servicio de administración de llaves Microsoft Azure Key Vault con los HSM certificados con FIPS 140-2 Nivel 3
- Identifique los ataques más rápidamente con el registro de acceso a datos a las aplicaciones SIEM líderes del sector
- Reduzca o elimine los riesgos derivados de las credenciales comprometidas con cifrado avanzado que incluye controles de acceso de usuario privilegiados
- Diseñe las aplicaciones para la nube con seguridad incorporada mediante tokenización sin bóveda con enmascaramiento dinámico de datos

‹Thales e-Security›

SOLUCIONES DE THALES E-SECURITY PARA MICROSOFT AZURE



ASEGURE LAS CARGAS DE TRABAJO A TRAVÉS DE NUBES HÍBRIDAS, INCLUIDAS MICROSOFT AZURE

Las cargas de trabajo de tecnología de la información en Microsoft Azure permiten ahorrar costos y obtener beneficios. Sin embargo, todavía necesita seguir las normas de seguridad, privacidad y cumplimiento, así como las mejores prácticas para proteger los datos. Además, se necesita una rápida movilidad de datos a través de todas las nubes que utilice ahora y en el futuro, una necesidad que puede verse comprometida con las soluciones de cifrado específicas del proveedor de la nube. Las soluciones de seguridad de Thales le ayudan a satisfacer estas necesidades con un cifrado avanzado y una administración centralizada de llaves que le proporcionan seguridad y control sobre los datos almacenados en sus instalaciones, en Microsoft Azurey en otros proveedores de la nube.

Los clientes que usan Microsoft Azure pueden administrar las llaves de cifrado de Azure Key Vault con los módulos de seguridad de hardware Thales nShield.

Microsoft Azure

SOLUCIONES DE THALES E-SECURITY PARA MICROSOFT AZURE

CIFRADO AVANZADO PARA LAS CARGAS DE TRABAJO DE MICROSOFT AZURE Y MÁS ALLÁ

Si su sistema está 100% basado en Microsoft Azure con rigurosos controles de seguridad internos o del sector, o si trabaja en nubes híbridas con datos distribuidos a través de su nube privada local, varios proveedores de nube y Microsoft Azure, necesita una solución de cifrado avanzada. Vormetric Transparent Encryption de Thales e-Security protege sus archivos y bases de datos almacenados en cualquier lugar, incluido Microsoft Azure, sin cambios en aplicaciones, bases de datos, infraestructura o prácticas empresariales. Vormetric Transparent Encryption para Microsoft Azure le permite:

- Reforzar la seguridad de los datos controlando el acceso no autorizado sobre la base de políticas de acceso de usuario granulares y con menos privilegios, incluida la identidad del usuario (incluidos los administradores con privilegios de raíz), el proceso, el tipo de archivo y la hora del día, entre otros
- Acelerar la detección de infracciones y cumplir los requisitos de cumplimiento con registros detallados de acceso a archivos. Se pueden dirigir los registros a la solución de administración de eventos e información de seguridad (SIEM) de su elección
- Obtener un retorno de la inversión más rápido con una implementación flexible y no intrusiva. Los agentes de cifrado operan en las instancias informáticas de Microsoft Azure o en cualquier otro servidor que acceda al almacenamiento y están disponibles para muchas versiones de Windows y distribuciones de Linux

ADMINISTRACIÓN DE LLAVES SEGURA Y CENTRALIZADA

Disponible en Microsoft Azure Marketplace, el administrador de seguridad de datos Vormetric Data Security Manager (DSM) proporciona una administración centralizada de llaves, para Vormetric Transparent Encryption para Microsoft Azure. El DSM está disponible como un dispositivo físico FIPS 140-2 Nivel 2 o 3 o un dispositivo virtual FIPS 140-2 Nivel 1.

CUMPLIMIENTO ACELERADO DE PCI-DSS

La tokenización Vormetric con enmascaramiento de datos dinámicos reduce el costo y el esfuerzo requeridos para cumplir con las políticas de seguridad y los requisitos regulatorios como el estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS). La tokenización asegura y anonimiza activos sensibles en el centro de datos, los entornos de datos grandes o la nube. La tokenización de preservación de formato protege los campos sensibles mientras mantiene la estructura de la base de datos, para una implementación no disruptiva.

Por ello, es fácil agregar a las aplicaciones enmascaramiento de datos dinámicos basados en políticas.

¡El servidor de tokenización Vormetric está disponible como un dispositivo virtual en el Microsoft Azure Marketplace!

TRAIGA SUS PROPIAS LLAVES AL SERVICIO DE ADMINSITRACIÓN DE LLAVES MICROSOFT AZURE

Los modules físicos de seguridad nShield de Thales (HSMs) combinan equipos informáticos probados en el campo, resistentes a la manipulación según validación FIPS 140-2 Nivel 3, con una arquitectura única de software que permite la escalabilidad líder en el sector y la conveniencia de administración de llaves. Los HSMs nShield le permiten llevar sus propias llaves a los servicios de administración de llaves Microsoft Azure Key Vault, lo que le da el control sobre las llaves de cifrado que protegen sus datos sensibles en la nube. Con nShield BYOK para Microsoft Azure, su nShield HSM en el local genera, almacena, envuelve y exporta llaves al servicio Microsot Azure Key Vault en su nombre. Los HSMs nShield están disponibles en tres variantes: con conexión a la red, con tarjeta PCIe y con conexión a USB, para adaptarse a sus requisitos de aplicación y necesidades de rendimiento. nShield BYOK para Microsoft Azure ofrece las siguientes ventajas:

- Prácticas de administración de llaves más seguras combinadas con los beneficios de escala, costo y conveniencia de la nube
- Mayor control sobre las llaves -usted maneja la generación de llaves, el almacenamiento y la exportación de las llaves utilizadas en el servicio Microsoft Azure Key Vault
- Generación de llaves fortalecida usando entropía nShield y equipos certificados por FIPS
- Administración de llaves local consistente para los principales proveedores de nube pública, incluidas Amazon Web Services y Google Cloud Platform

CUMPLA CON LOS REQUISITOS DE PROTECCIÓN DE DATOS

Thales e-Security simplifica la seguridad de las cargas de trabajo de Microsoft Azure para ayudarle a cumplir con las regulaciones de seguridad de datos internas, gubernamentales y del sector. Los productos de seguridad de datos Vormetric disponibles en el mercado Azure – Cirado Transparente y Tokenización - operan sin problemas en las cargas de trabajo de Microsoft Azure, los proveedores de servicios administrados y en sus instalaciones, proporcionando una administración centralizada de políticas y llaves. nShield BYOK para los servicios de administración de llaves Microsoft Azure Key Vault le brinda control sobre el cifrado para poder cumplir con los requisitos y proteger sus datos.

CONOZCA MÁS

Visítenos en **www.thalesesecurity.com** para conocer cómo nuestras soluciones y servicios avanzados de seguridad de datos brindan confianza dondequiera que se genere, comparta o almacene la información.

Siganos en:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com