FUTUREX

CryptoHub *Resumen de Solución*

LA PLATAFORMA CRIPTOGRÁFICA **TODO EN UNO** BASADA EN HARDWARE

Dinámica Solución para Resolver la Expansión Criptográfica

Simplificar la complejidad de la criptografía en la infraestructura es crucial para la ciberseguridad. Muchas organizaciones enfrentan desafíos al implementar y administrar soluciones de varios proveedores. Esta complejidad, originada por las adquisiciones en el sector, presenta obstáculos tanto evidentes como ocultos, a pesar del objetivo de una solución unificada.

CryptoHub destaca como la única plataforma criptográfica todo en uno del sector, construida sobre una base de código común. Esta ventaja singular reduce notablemente el tiempo necesario para implementar servicios criptográficos, superando a las soluciones rivales en más del 90%.

La infraestructura criptográfica convencional implica la utilización de múltiples productos de diferentes proveedores, lo que requiere conocimientos especializados y costosos, así como servicios de integración y mantenimiento onerosos. Este enfoque simplemente no es viable para las empresas modernas.

CryptoHub está disponible como dispositivo local, instancia en la nube en contenedores o a través de VirtuCrypt SaaS de Futurex, con 13 centros de datos en todo el mundo. Esto facilita el despliegue instantáneo y la integración sin problemas, permitiendo a las organizaciones aprovisionar dinámicamente cualquier solución criptográfica, ya sea de pago o de uso general, según la demanda.

El Reto de los Sistemas Heredados

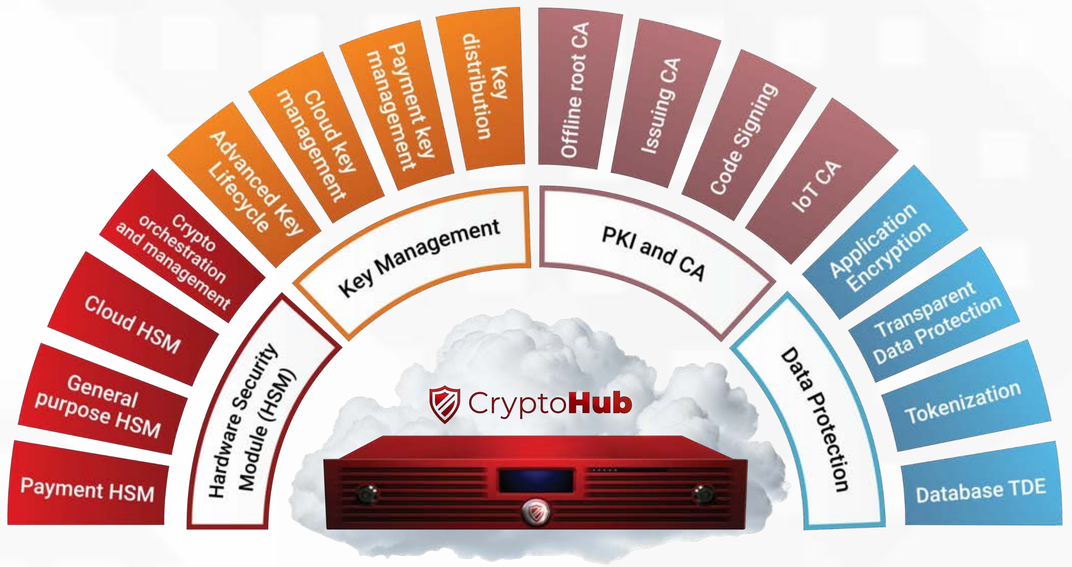
Los sistemas criptográficos heredados se basan en soluciones fragmentadas, requiriendo módulos de seguridad de hardware (HSM) independientes para la protección de datos y seguridad de pagos, así como sistemas separados para funciones estándar como PKI y CA. Este enfoque fragmentado genera complejidades de integración, vulnerabilidades de seguridad e ineficiencias operativas, obstaculizando la capacidad de las organizaciones para hacer frente a las amenazas cibernéticas modernas.

CryptoHub resuelve esta proliferación criptográfica al consolidar todas estas funcionalidades en una plataforma unificada. Al adoptar CryptoHub, las organizaciones experimentan una simplicidad, seguridad y escalabilidad sin precedentes. Esta solución no solo mejora la eficiencia operativa y agiliza las operaciones actuales, sino que también prepara el terreno para estrategias futuras de protección de datos al ofrecer una única solución para diversas necesidades criptográficas.

Los líderes de TI visionarios están adoptando CryptoHub como una inversión estratégica, desbloqueando un cifrado integral que se adapta a la evolución de las amenazas cibernéticas para garantizar una sólida protección de los datos.

Soluciones CryptoHub

La plataforma CryptoHub se basa en cuatro pilares fundamentales: Módulos de seguridad de hardware (HSM), gestión de llaves, PKI y autoridad de certificación, y protección de datos. Cada uno de ellos proporciona la seguridad, eficiencia y escalabilidad sin precedentes que requiere el panorama actual de la ciberseguridad, al tiempo que conserva las características distintivas de la plataforma unificada CryptoHub, que garantiza una gestión simplificada y la orquestación criptográfica.



Hardware Security Modules (HSM)

La serie CryptoHub HSM ofrece soluciones de clase empresarial tanto para aplicaciones de uso general como de pago, todo dentro de una sola plataforma, asegurando así el más alto nivel de seguridad para una variedad de casos de uso. Con una capacidad para procesar más de 100,000 transacciones por segundo (TPS), brinda un rendimiento excepcional sin comprometer la seguridad. Cada HSM se somete a rigurosas pruebas y certificaciones para cumplir con las normativas reglamentarias, incluyendo estándares como FIPS 140-2 Nivel 3 y PCI HSM, garantizando así el cumplimiento normativo y la tranquilidad de las organizaciones.

Una de las características más destacadas de los HSM de CryptoHub es su compatibilidad con todas las API y bibliotecas criptográficas de uso general y de pago, incluyendo interfaces como PKCS #11, Java, CNG y RESTful. Esta amplia compatibilidad asegura una integración perfecta con los sistemas y aplicaciones existentes, permitiendo a las organizaciones aprovechar al máximo la potencia de nuestros HSM sin interrupciones.

Los HSM CryptoHub introducen innovadoras capacidades de segmentación mediante HSM virtuales, que particionan de forma segura las cargas de trabajo de las aplicaciones. Cada HSM virtual opera de manera independiente, con sus propias llaves maestras y políticas de seguridad, garantizando así el aislamiento y mejorando la postura de seguridad.

Además, los HSM CryptoHub minimizan el tiempo de inactividad y aseguran la disponibilidad continua de los servicios criptográficos mediante redundancia y conmutación por error. Esto se logra mediante fuentes de alimentación y puertos Ethernet dobles y redundantes, que permiten un funcionamiento ininterrumpido, junto con la sincronización automática de la información del dispositivo para facilitar una conmutación por error instantánea.

Manejo de Llaves

En el núcleo de CryptoHub radica un sistema de gestión de llaves sofisticado, que orquesta con precisión y fiabilidad la generación, almacenamiento, distribución y destrucción de llaves criptográficas. Este sistema agiliza las operaciones de gestión de llaves al eliminar la necesidad de múltiples productos heterogéneos y conocimientos especializados. Al consolidar estas funciones en una plataforma unificada, CryptoHub mejora la eficiencia operativa y reduce considerablemente los costos asociados con la integración y el mantenimiento, estableciendo así un nuevo estándar en soluciones de seguridad criptográfica.

El aprovisionamiento dinámico de CryptoHub, impulsado por el hipervisor HSM de Futurex, facilita el despliegue rápido de llaves maestras HSM virtuales (VMK) y la creación de grupos en clústeres entre regiones, garantizando un tiempo de actividad máximo y una escalabilidad óptima. CryptoHub simplifica tanto la implementación como la gestión de bloques de llaves, incluyendo la normativa KBPK X9.143. Las diversas opciones de despliegue de CryptoHub, que van desde dispositivos físicos a virtuales, pasando por contenedores, e incluso un servicio personalizable (KMaaS - Key Management as a Service), se adaptan a las variadas necesidades empresariales y preferencias de infraestructura.

La robusta seguridad de nivel empresarial de CryptoHub se respalda con su conformidad a los principales estándares de la industria, como FIPS 140-2 Nivel 3, PCI DSS y PCI HSM. Además, CryptoHub destaca por su liderazgo en la inyección flexible de llaves, ofreciendo soporte para capacidades únicas como llave clara, llave de carga útil cifrada e inyección remota de llaves, cumpliendo así de manera excepcional con el control de PIN 32.9 de la PCI para la carga remota de llaves cifradas.

Con su compatibilidad con una amplia variedad de bibliotecas criptográficas, API y protocolos, CryptoHub garantiza una integración sin fisuras en los ecosistemas criptográficos existentes.

En resumen, las capacidades de gestión de llaves de CryptoHub encarnan la excelencia en seguridad criptográfica, proporcionando a las organizaciones la confianza y las herramientas necesarias para proteger sus activos más valiosos en un entorno de amenazas en constante evolución.

PKI y Certificate Authority

CryptoHub ofrece una solución completa de PKI y autoridad de certificación, permitiendo a las organizaciones establecer CA raíz fuera de línea, emitir certificados, realizar firma de código y gestionar certificados IoT de manera sencilla.

Con CryptoHub, las organizaciones pueden gestionar su infraestructura PKI de forma segura, garantizando la integridad y autenticidad de los certificados digitales. Las CA raíz fuera de línea reducen el riesgo de compromiso al salvaguardar la raíz de confianza de manera offline. Además, las capacidades de emisión de certificados de CryptoHub permiten una emisión eficiente para diversos casos de uso, mientras que las funciones de firma de código aseguran la autenticidad e integridad del software.

La funcionalidad IoT CA de CryptoHub simplifica la gestión de certificados para dispositivos IoT, garantizando una comunicación y autenticación seguras. Esto permite a las organizaciones establecer y mantener una sólida infraestructura PKI, asegurando transacciones y comunicaciones digitales seguras.

Las capacidades PKI y CA de CryptoHub son fundamentales para las infraestructuras de comunicación seguras, facilitando la autenticación mutua y el cifrado de datos entre entidades. Al aprovechar las funcionalidades de CA raíz offline y CA emisora de CryptoHub, las organizaciones pueden establecer jerarquías de confianza de certificados digitales, garantizando la integridad y autenticidad de las transacciones digitales.

La versatilidad de CryptoHub lo hace adaptable a diversos casos de uso, desde entornos empresariales tradicionales hasta ecosistemas emergentes de IoT. Las funcionalidades PKI y CA de CryptoHub ofrecen flexibilidad y escalabilidad sin precedentes, protegiendo transacciones de pago, firmando código para la integridad del software y proporcionando certificados para dispositivos IoT.

Además, la compatibilidad de CryptoHub con la firma de código permite a los equipos DevOps optimizar las capacidades CI/CD para proteger su propiedad intelectual mediante la firma digital de ejecutables y actualizaciones de firmware, mitigando así el riesgo de manipulación o modificaciones no autorizadas.

En el cambiante panorama de la ciberseguridad, CryptoHub se destaca con su compromiso con el cumplimiento de normas y la innovación. Con certificaciones como FIPS 140-2 Nivel 3 y PCI HSM, CryptoHub garantiza que la infraestructura criptográfica cumple estrictos requisitos de seguridad.

En resumen, las capacidades de PKI y CA de CryptoHub proporcionan a las organizaciones una base sólida para la comunicación segura y la gestión de identidades.

Protección de Datos

Las capacidades de protección de datos de CryptoHub abarcan una amplia gama de técnicas de cifrado avanzadas diseñadas para asegurar los datos en reposo, en tránsito y durante el procesamiento. Desde el cifrado de aplicaciones hasta la protección transparente de datos, la tokenización y el TDE (Transparent Data Encryption) de bases de datos, CryptoHub ofrece a las organizaciones un sólido marco para mitigar los riesgos asociados con las filtraciones de datos y los accesos no autorizados.

La funcionalidad de cifrado de aplicaciones de CryptoHub mejora la seguridad al cifrar los datos de las aplicaciones antes de su almacenamiento o transmisión, integrándose perfectamente con las aplicaciones existentes. Esto garantiza que los datos permanezcan protegidos incluso en caso de infracción, minimizando el impacto potencial en las operaciones empresariales y la confianza de los clientes.

La protección de datos transparente de CryptoHub cifra los datos a nivel del sistema de archivos o del disco, asegurando que la información confidencial permanezca a salvo de accesos no autorizados. Este enfoque minimiza la sobrecarga de rendimiento normalmente asociada al cifrado, permitiendo a las organizaciones mantener un rendimiento óptimo del sistema mientras cumplen con las normas de seguridad.

La tokenización, incluida la tokenización sin bóveda, es una característica esencial de CryptoHub que permite a las organizaciones intercambiar datos confidenciales por tokens no confidenciales, reduciendo significativamente el riesgo de filtración de datos al sustituir información crítica como números de tarjetas de crédito o PII por tokens. La adopción de la tokenización sin bóveda garantiza el cumplimiento normativo y protege a las organizaciones de los efectos perjudiciales de las filtraciones de datos en las operaciones y la reputación empresarial.

La funcionalidad de TDE de bases de datos de CryptoHub proporciona a las organizaciones una solución robusta para cifrar los datos almacenados en bases de datos, asegurando que la información sensible permanezca protegida contra accesos no autorizados. Al cifrar los datos de forma transparente a nivel de base de datos, CryptoHub permite a las organizaciones cumplir con los requisitos normativos y proteger la información sensible de amenazas internas y externas.

En resumen, las capacidades de protección de datos de CryptoHub ofrecen a las organizaciones un completo marco para salvaguardar la información sensible en toda la empresa.

Resumen Ejecutivo

CryptoHub está transformando la seguridad de los datos con su conjunto integrado de servicios criptográficos. Con potentes módulos de seguridad de hardware (HSM), gestión avanzada de llaves, PKI y CA completos, y sólidas capacidades de protección de datos, CryptoHub asegura una protección integral para organizaciones de todo el mundo.

Al aprovechar la potencia de CryptoHub, las empresas pueden fortalecer sus defensas de datos y mantener la confianza con una eficiencia y flexibilidad sin precedentes, respaldadas por una serie de certificaciones líderes en el sector. Con CryptoHub, el futuro de la seguridad de los datos no solo está asegurado, sino que se eleva a nuevas alturas de fiabilidad y resistencia.

Obtén más información en www.futurex.com/cryptohub.

FUTUREX

Desde hace más de 40 años, Futurex ha sido un líder e innovador galardonado en el mercado del cifrado, ofreciendo soluciones de seguridad de datos de nivel empresarial con los más altos estándares de protección. Más de 15.000 organizaciones de todo el mundo confían en Futurex para obtener soluciones de vanguardia que incluyen módulos de seguridad de hardware preparados para la criptografía poscuántica (PQC), gestión de llaves, infraestructura de llave pública (PKI) y autoridades de certificación (CA), protección de datos y HSM en la nube.

Futurex tiene su sede en las afueras de San Antonio, Texas, y cuenta con oficinas regionales en todo el mundo y más de una docena de centros de datos distribuidos en cinco continentes. Futurex ofrece un soporte inigualable para satisfacer las necesidades de cifrado de datos y gestión de llaves esenciales para las operaciones de sus clientes.

FUTUREX.COM

864 Old Boerne Road,
Bulverde, Texas 78163