Libere todo el potencial del cifrado conquistando la gestión de claves

VaultCore™ de Fornetix® es una solución de ciberseguridad hiperescalable que automatiza la criptografía para la protección dinámica de activos.

FORNETIX VAULTCORE

Escalabilidad

Almacena cientos de millones de claves - órdenes de magnitud por encima de los tolos existentes

Automatización

Programe y ejecute operaciones criptográficas en millones de claves a la vez

Compatibilidad

Integración perfecta con las inversiones tecnológicas heredadas, existentes y futuras

Cumplimiento

Permita la elaboración de informes y auditorías completas para las regulaciones actuales, que son cada vez más numerosas

A MEDIDA QUE LAS BRECHAS DE DATOS SE CONVIERTEN EN UN ACONTECIMIENTO CASI DIARIO, ES FUNDAMENTAL QUE LA INFORMACIÓN QUE REQUIERE ENCRIPTACIÓN ESTÉ PROTEGIDA EN SU CREACIÓN, EN SU USO, EN TRÁNSITO Y EN REPOSO.

Los métodos de despliegue y gestión de las claves de cifrado en diversos dispositivos y sistemas han adoptado tradicionalmente un enfoque ascendente. Este flujo de control dispar conduce a una falta de encriptación plenamente utilizada, a averías en las redes que requieren encriptación y a una gestión inadecuada de las claves de encriptación. El resultado es que se utilizan múltiples sistemas o procesos manuales dentro de la misma organización para crear y distribuir claves de cifrado a sistemas aislados que pueden utilizar una variedad de gestores de claves de cifrado. El nivel de encriptación y la adopción de métodos para desplegar claves de encriptación varía entre las industrias en función de las necesidades, las tecnologías en uso y los tipos de dispositivos que utilizan la encriptación.

Fornetix reconoce el valor y la necesidad que tienen las empresas, organizaciones y proveedores de servicios de proteger la información crítica, permitir transacciones comerciales seguras y ofrecer servicios de confianza para garantizar la seguridad y confidencialidad de sus clientes y socios comerciales.

Las mejores prácticas para la gestión de sistemas empresariales son los métodos descendentes y centralizados. Aunque hoy en día existen muchos productos y soluciones diferentes que crean claves de cifrado para las organizaciones, el reto consiste en encontrar un enfoque que proporcione una escalabilidad práctica y asequible.

Hasta ahora no existían opciones para gestionar, distribuir y federar fácilmente las claves de cifrado combinadas con la necesaria conformidad con las políticas de la organización. Las metodologías existentes suelen ser propietarias y específicas para cada dispositivo. Este enfoque no admite el control centralizado de las aplicaciones, las comunicaciones y la infraestructura de la empresa.

Afortunadamente, ahora existe una solución moderna y escalable...

© 2021 Fornetix

Centralice la gestión de claves con VaultCore de Fornetix

VaultCore (VC) resuelve estos retos centrándose en la gestión, distribución y federación de claves de cifrado. VaultCore ayuda a coordinar las actividades del ciclo de vida de las claves de cifrado con las aplicaciones, las comunicaciones y la gestión de la infraestructura.

Al coordinar estos recursos con el resto de la empresa, la supervisión de la utilización de las claves se alinea con otros componentes de la política, la supervisión de la empresa y las funciones de gestión. Esto hace que el cifrado sea más accesible y lo hace funcionar como un servicio. La gestión de c laves se convierte entonces en un componente integral de la gestión de la misión, situando el cifrado en línea con otros aspectos de los entornos de datos y comunicaciones seguros.

El cifrado debe gestionarse de arriba abajo para garantizar que se sigue la política de la organización y que las claves se generan y distribuyen de forma segura dentro del ámbito de control de la organización. Para lograr este objetivo, se necesita un método estándar que organice la comunicación de las operaciones de gestión de claves en un contrato de datos, de modo que las aplicaciones de gestión puedan controlar los dispositivos inscritos y éstos puedan recibir y solicitar material de claves de forma automatizada.

FORNETIX VAULTCORE

Compromiso con las normas: Un camino hacia el futuro

VaultCore aprovecha el Protocolo de Interoperabilidad de Gestión de Claves (KMIP), los Estándares de Criptografía de Clave Pública #11 (PKCS#11) y el Formato Común de Eventos (CEF) como enfoques basados en estándares para la gestión de claves, el comando y control, la integración de módulos de seguridad de hardware y la integración de la gestión de eventos de seguridad (SIEM). KMIP y PKCS#11 son especificaciones técnicas definidas por la Organization for Advancement of Structured Information Standards (OASIS). Tanto KMIP como PKCS#11 están directamente asociados a los estándares proporcionados por el Instituto Nacional de Estándares y Tecnología (NIST).

A medida que cosas como la criptografía cambian con el tiempo, el compromiso con los estándares se convierte en una puerta de transición, dando a los usuarios de VaultCore la capacidad de abordar el cambio a escala empresarial con seguridad y eficiencia.

La funcionalidad de VaultCore se basa en proporcionar interoperabilidad, extensibilidad, escalabilidad y seguridad a nivel empresarial. El énfasis en estas cualidades proporciona un marco para la seguridad centrada en los datos que beneficia a una organización al alinear los controles con el flujo de información en la empresa. Al alinear los controles de seguridad basados en el cifrado, la definición de la autorización y la gestión con el negocio de una organización, es posible aplicar la idea de que la "necesidad de conocer" debe seguir un proceso estricto.

Al considerar las necesidades de seguridad centradas en los datos de su organización, el énfasis en la interoperabilidad, la extensibilidad, la escalabilidad y la seguridad hacen de VaultCore una solución que le permite liberar todo el potencial del cifrado.

Interoperabilidad

La tecnología de Fornetix se rige por el lema "en los estándares confiamos". Esto proporciona una base sólida para la extensibilidad y define los límites que afectan a cuánto puede crecer VaultCore (escalabilidad) y cómo VaultCore proporciona protección a los sistemas externos (seguridad). El motor de políticas de VaultCore es un punto de decisión para las operaciones criptográficas que utiliza el lenguaje de los estándares conocidos como base para la definición de políticas.

Además, los ingenieros de Fornetix están ayudando a forjar la próxima generación de estándares sirviendo activamente en grupos de la industria como el Comité Técnico de KMIP. Fornetix es uno de los principales participantes en el ejercicio anual de interoperabilidad de OASIS, con resultados sistemáticamente buenos.

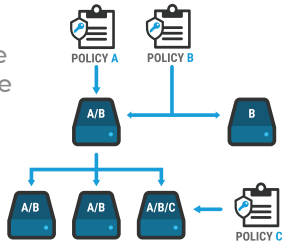
PRINCIPALES CARACTERÍSTICAS DE LA INTEROPERABILIDAD DE VAULTCORE

- Interfaz KMIP totalmente compatible: KMIP 1.0-1.4
- Servicios KMIP a través de TTLV, HTTPS, JSON y XML
- Registro CEF para soportar una rápida integración SIEM
- Capacidad de reenviar operaciones KMIP a otros gestores de claves compatibles con KMIP
- Interfaz PKCS#11 para la integración de HSM para proteger el almacén de claves VC
- Cifrar y gestionar máquinas virtuales mediante la interoperabilidad con VMware vSphere y vSAN

© 2021 Fornetix

Extensibilidad

La posibilidad de ampliar la capacidad manteniendo un entorno altamente interoperable y seguro es una característica clave de VaultCore. Esta característica incluye la integración de la gestión de claves con otros sistemas mediante la traducción de protocolos (NETCONF, F5, Microsoft Cryptographic Next Generation APIs) para apoyar la consolidación de las interfaces de usuario y soportar una defensa de red dinámica y adaptable que incluya la seguridad de los datos en reposo y en movimiento.



PRINCIPALES CARACTERÍSTICAS DE LA EXTENSIBILIDAD DE VAULTCORE

- Servicios RESTful para integrar VaultCore con los servicios empresariales existentes
- Scripts personalizados de VaultCore para automatizar operaciones complejas de cifrado y gestión de claves
- Programación de VaultCore para ejecutar scripts de automatización
- Orquestadores de Windows y Linux para la traducción de protocolos basada en KMIP de los servicios de Microsoft, autoridades de certificación, NETCONF y otros protocolos
- VaultCore Policy para definir reglas de autorización fuera de las operaciones de gestión de claves

Escalabilidad

VaultCore tiene la capacidad de soportar cientos de millones de claves mientras soporta redes móviles adhoc, comunicaciones tácticas y encriptación de archivos u objetos. Las composiciones y trabajos de VaultCore dan a las organizaciones la capacidad de definir operaciones complejas de gestión de claves en bloque.Esto permite a los clientes orquestar la gestión de claves, el cifrado, la seguridad de la red y los sistemas empresariales con la garantía de que las claves utilizadas están seguras y no se perderán.

PRINCIPALES CARACTERÍSTICAS DE LA ESCALABILIDAD DE VAULTCORE

- El almacén de datos VaultCore está diseñado para mantener un repositorio de cientos de millones de claves
- Alta disponibilidad y copias de seguridad completas utilizando la replicación cifrada con dispositivos VC geo-separados para garantizar que nunca se pierdan las claves
- Posibilidad de integrar módulos de seguridad de hardware (HSM) integrados o basados en la red para proteger los almacenes de claves en una configuración de alta disponibilidad
- Estructura de precios que anima -no penaliza- a las organizaciones a utilizar el mayor número de claves posible

Seguridad

VaultCore permite controles de acceso obligatorios a través de la seguridad posicional y la política. Los controles de acceso discrecionales a través de la agrupación KMIP permiten al servidor VaultCore proporcionar un ciclo de vida de claves seguro desde el centro de datos hasta el borde táctico.

PRINCIPALES CARACTERÍSTICAS DE LA SEGURIDAD DE VAULTCORE

- Los dispositivos VaultCore se ejecutan con SELinux en modo de refuerzo para proteger los procesos en ejecución y aplicar comportamientos estrictos
- Roles de usuario para la gestión de claves y políticas que permiten la separación de controles entre la gestión de claves y la gestión de políticas
- El motor de políticas de VaultCore permite definir servicios de puntos de decisión criptográficos para la integridad bipersonal a escala de IoT
- Conexiones TLS mutuas para la distribución de claves, objetos de gestión, política efectiva e instrucciones de orquestación
- La seguridad posicional aplica controles de acceso obligatorios en función del lugar en el que se asocia una determinada conexión de cliente en la jerarquía de VC
- Cada dispositivo VC utiliza unidades de autocifrado con certificación FIPS para garantizar la seguridad de los datos si se retira físicamente una unidad
- Módulos de seguridad de hardware disponibles para proteger los almacenes de claves en configuraciones independientes y de alta disponibilidad
- The entirety of VaultCore is owned, designed, assembled, and in the U.S. to comply with the Buy American Act

© 2021 Fornetix

Opciones de despliegue

Desde pequeños negocios hasta empresas globales con infraestructura masiva de IoT, hay una solución de despliegue de VaultCore que satisface perfectamente las necesidades únicas de su organización. VaultCore está diseñado para crecer con usted a medida que su uso de cifrado aumenta. Un pequeño despliegue de dispositivos VaultCore basados en software puede actualizarse rápidamente y sin problemas a la potencia y capacidad líderes en la industria de nuestros dispositivos de hardware montados en rack. El VCH-2000H incluye un módulo de seguridad de hardware (HSM) incrustado dentro del chasis para el cumplimiento del nivel 3 de FIPS 140-2 con la raíz de confianza HSM.

Dispositivos de hardware

FUENTE DE ALIMENTACIÓN

VCH-1000	2-750w hot-swap
VCH-2000	2-1000w hot-swap
VCH-2000H	2-1000w hot-swap

CHOQUE

Choque Prueba de caída	12G, -3.75G

INTERFACES

6 puertos de cobre RJ45 de 1 GB
VCH-1000: 2 ranuras de actualización de red opcionales
VCH-2000: 6 ranuras de actualización de red opcionales
VCH-2000H: 6 ranuras de actualización de red opcionales
Interfaz gráfica de usuario (GUI)
API KMIP
Interfaz de línea de comandos
Cliente VaultCore, agente y servicios RESTful
HSM (PKCS #11)

CAPACIDAD DE CLAVES

VCH-1000	10,000,000
VCH-2000	100,000,000+
VCH-2000H	100,000,000+

CERTIFICACIONES E INTEROPERABILIDAD

VCH-1000 - Cumple con FIPS 140-2 Nivel 2
VCH-2000 - Certificado FIPS 140-2 Nivel 2 (Ver Certificación)
VCH-2000H - FIPS 140-2 Nivel 3 con HSM raíz de confianza
Compatible con KMIP 1.0, 1.1, 1.2, 1.3 y 1.4

ESCALABILIDAD Y CONMUTACIÓN POR ERROR

Totalmente distribuible

Soporte de clustering

Alta disponibilidad / cero interrupción de la conmutación por error

Proceso de copia de seguridad/restauración

Dispositivos virtuales

CPU VIRTUAL

VCV-100	2 CPU
VCV-500 (Discovery Edition)	2 CPU
VCV-500	2 CPU

MEMORIA VIRTUAL

VCV-100	4GB RAM
VCV-500 (Discovery Edition)	4GB RAM
VCV-500	4GB RAM

ALMACENAMIENTO VIRTUAL

VCV-100	16GB
VCV-500 (Discovery Edition)	16GB
VCV-500	16GB

CAPACIDAD CLAVE

VCV-100	125,000
VCV-500 (Discovery Edition)	250,000
VCV-500	250,000

CERTIFICACIONES E INTEROPERABILIDAD

Cumple con FIPS 140-2 Nivel 1
Compatible con KMIP 1.0, 1.1, 1.2, 1.3 y 1.4

ESCALABILIDAD Y CONMUTACIÓN POR ERROR

Totalmente distribuible
Soporte de clustering
Alta disponibilidad / cero interrupción de la conmutación por error
Proceso de copia de seguridad/restauración

INTERFACES

Graphical User Interface (GUI)
KMIP API
Command Line Interface
VaultCore Client, Agent, and RESTful Services
HSM (PKCS #11)

Fornetix.com Linkedin.com/company/fornetix Twitter.com/fornetix Facebook.com/fornetix 1-844-539-6724 5123 Pegasus Ct, Suite X, Frederick, MD 21704

© 2021 Fornetix