

¿Qué es Kinamik Secure Audit Vault?

Kinamik Secure Audit Vault es una solución software que recoge, asegura y centraliza en tiempo real los registros de auditoría desde diversas fuentes. En el momento en que éstos son generados les aplica un sello digital que permite evidenciar cualquier manipulación, obteniendo así pruebas irrefutables de su integridad.

Facilita la reducción de costes asociados a procesos de auditoría y cumplimiento de leyes, a la vez que mitiga la amenaza interna y fortalece su validez legal para ser usados como prueba electrónica en caso de litigio.

¿Qué beneficios se obtienen con Kinamik Secure Audit Vault?

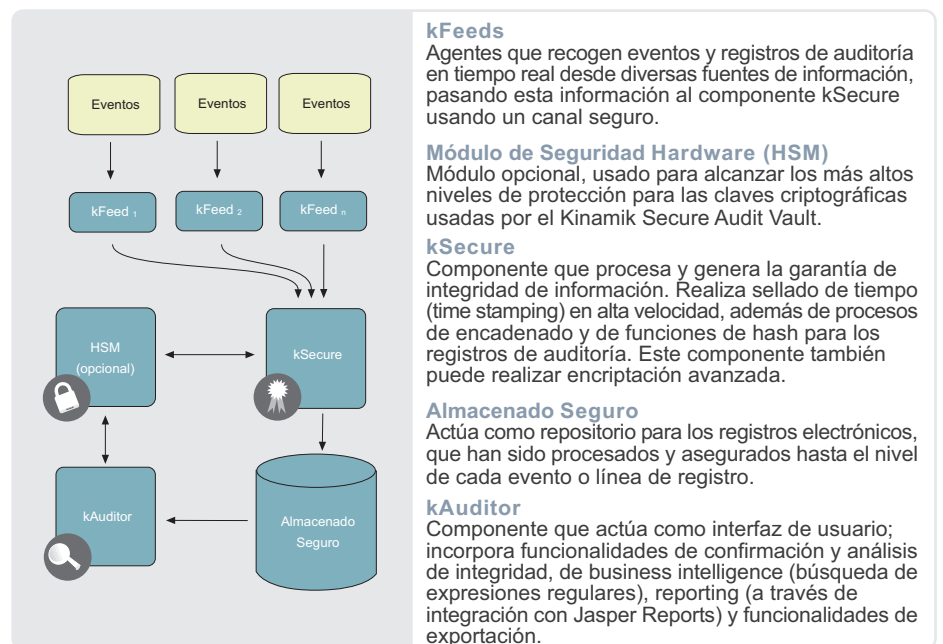
- ▶ Reduce costes asociados a procesos de gobernabilidad, gestión de riesgos y cumplimiento de normativas (GRC)
- ▶ Reduce costes asociados a procesos de auditoría, gestión de pruebas electrónicas (e-discovery) y procesos de investigación de informática forense
- ▶ Disuade el fraude y reduce el riesgo e impacto de la amenaza interna. Establece una mayor transparencia y permite rendir cuentas a todos y cada uno de los usuarios, (incluso a los administradores)
- ▶ Apoya procesos judiciales al aumentar el poder probatorio de los registros electrónicos
- ▶ Cumple y ayuda a cumplir las más exigentes leyes, buenas prácticas y estándares internacionales en lo que respecta a la prevención y detección de manipulación de registros electrónicos (por ej. PCI-DSS, NIST, etc.)

¿Puede usted confiar en sus registros electrónicos, especialmente aquellos bajo amenaza interna, usados como prueba electrónica o en el ámbito de leyes y normativas?

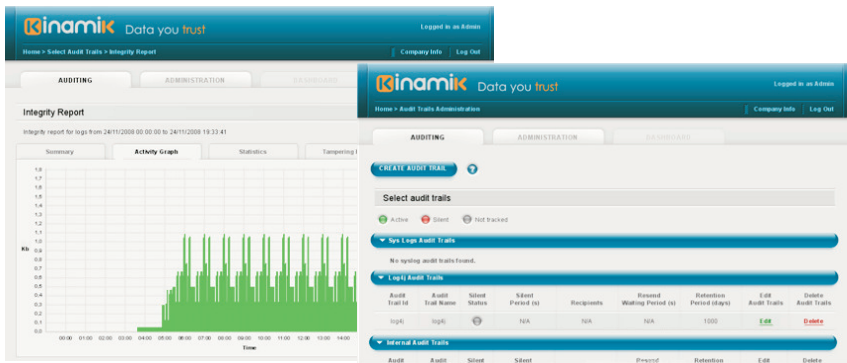
La correcta gestión de la información, la eficaz gestión de riesgos y el efectivo cumplimiento de normativas y leyes son necesidades importantes que las organizaciones deben hacer frente. Estos esfuerzos representan un desafío creciente para las empresas: es cada vez más difícil y costoso cumplir con los mandatos; la amenaza interna va en aumento; y seguir los requerimientos asociados a la gestión, presentación y aceptación de pruebas electrónicas es cada vez más complicado y caro.

Kinamik Secure Audit Vault hace frente a estos desafíos al ofrecer una bóveda centralizada y segura para todos los registros de auditoría. Simplifica las tareas de archivo, preservación y búsqueda de información, al tiempo que mantiene los registros en forma segura, procesándolos para alcanzar los más altos niveles de integridad. Kinamik Secure Audit Vault es capaz de manejar sin sobresaltos una gran cantidad de información desde diferentes fuentes, incluyendo aplicaciones, bases de datos, servidores y dispositivos conectados a redes. Los registros preservados en la bóveda de Kinamik Secure Audit Vault se encuentran en formato nativo (*raw*), han sido securizados a nivel de cada evento y se les ha aplicado un sello de inviolabilidad, pudiendo demostrar en forma fehaciente e irrefutable si algún registro ha sido manipulado. Usando una interfaz web, Kinamik Secure Audit Vault permite buscar y analizar en los registros preservados según necesidad.

Al mantener una plataforma centralizada y segura para los registros de auditoría, Kinamik Secure Audit Vault facilita y contribuye a reducir los costes asociados a procesos de cumplimiento de leyes; favorece la disminución del riesgo de ataques internos al proveer información irrefutable de toda la actividad realizada, incluso por parte de usuarios con altos privilegios; finalmente, apoya procesos judiciales al otorgar pruebas incuestionables de la integridad de los registros de auditoría que serán utilizados como prueba electrónica.



Kinamik Secure Audit Vault · Arquitectura de Producto



Kinamik Secure Audit Vault · Gráfica de actividad del Integrity Report y Consola de Administración

Características técnicas y funcionalidades

- ▶ Agentes de recolección de datos: los agentes de Kinamik Secure Audit Vault recogen y transmiten datos en tiempo real a través de un canal seguro encriptado.
- ▶ Compresión de mensajes en tránsito: reduzca el tráfico en red mediante la compresión de hasta el 70% en el tamaño de los mensajes enviados al componente de sellado digital para la protección de integridad.
- ▶ Encriptación de datos opcional: todos los datos residentes en la bóveda segura de auditoría pueden ser transformados en confidenciales utilizando protocolos estándar de encriptación.
- ▶ Gestión de usuario por LDAP: Kinamik Secure Audit Vault se integra con los sistemas de gestión de usuarios y es compatible con LDAPv3 y Active Directory.
- ▶ Uso de Autoridades de Sellado de Tiempo (TSA) externas: Kinamik Secure Audit Vault es compatible con Autoridades de Sellado de Tiempo (TSA), elevando el nivel de seguridad y protección de la integridad.
- ▶ Herramienta de política de retención de datos: defina en forma independiente diferentes políticas de retención para cada fuente de información, cumpliendo así con los periodos específicos de retención exigidos por diversas leyes, regulaciones y estándares (por ej. PCI-DSS, HIPAA, Basel II, SOX, MiFID, etc.)
- ▶ Búsqueda expresiones regulares: utilice las capacidades de búsqueda del Kinamik Secure Audit Vault para localizar de forma precisa y exacta cadenas de texto y expresiones en los datos securizados.
- ▶ Informe de integridad de los datos: evalúe el nivel de confianza de los datos con una sencilla verificación usando la herramienta de análisis de integridad. Señala de forma precisa a nivel de evento o línea de registro cualquier tipo de alteración o modificación que afecte la integridad de la información.
- ▶ Capacidades de compresión para almacenamiento y archivado: reduzca costes de almacenamiento y archivado de información sensible usando las funcionalidades de compresión del Kinamik Secure Audit Vault, alcanzando ratios de compresión de hasta 5:1.
- ▶ Fácil integración con herramientas de reporting (Jasper Reports): exporte fácilmente los resultados de verificación de la integridad a algunas de las soluciones de business intelligence líderes en el mercado.
- ▶ Alto rendimiento: la tecnología de sellado del Kinamik Secure Audit Vault es capaz de procesar y securizar hasta 40.000 EPS (eventos por segundo)*

* Capacidad de firma de kSecure. Los resultados pueden variar dependiendo de factores tales como la configuración del sistema.

Acerca de Kinamik Data Integrity



El software de Kinamik Data Integrity protege la manipulación de los registros digitales. Construimos en tiempo real una Bóveda de Auditoría Centralizada para registros de auditoría con integridad y autenticidad al más alto nivel de granularidad posible, creando en el mundo digital niveles de evidencia similar al de los registros tradicionales basados en papel. Kinamik disuade, detecta y demuestra cualquier manipulación para garantizar que la información digital sea correcta.

Nuestra misión es elevar el nivel de confianza en las organizaciones, facilitar la rendición de cuentas y asegurar la privacidad en industrias que trabajen con grandes volúmenes de información sensible.

Kinamik es Sun Startup Essential Partner y Oracle Partner.

Se han realizado todos los esfuerzos posibles para asegurar que la información incluida en este folleto es precisa y está actualizada en el momento de ser publicada. No obstante, Kinamik se reserva el derecho de modificar las especificaciones en cualquier momento. El contenido de este documento no representa ninguna obligación contractual, directa o indirecta. Kinamik es una marca de Kinamik Data Integrity, S.L. El resto de marcas incluidas en el documento son propiedad de sus respectivos propietarios.

© 2010, Kinamik Data Integrity S.L.

Arquitectura

- ▶ Arquitectura de 3 capas
- ▶ J2EE + Spring
- ▶ Totalmente clusterizable

Algoritmos criptográficos soportados

- ▶ Encriptación: AES 256, RSA - 1024+
- ▶ Hashing: SHA-256, SHA-512 y posterior

Plataformas soportadas

- ▶ Linux/UNIX
- ▶ Solaris
- ▶ Windows
- ▶ Cualquier sistema operativo que soporte Java

Fuentes soportadas

- ▶ Mensajes Syslog (UDP)
- ▶ Ficheros de texto
- ▶ Aplicaciones JDBC
- ▶ Log4J (aplicaciones ejecutadas sobre una JVM 1.4 o posterior)
- ▶ Registros de auditoría de BEA Weblogic 9
- ▶ Registros de Auditoría OpenSolaris
- ▶ Nuevas plataformas están siendo constantemente añadidas, y pueden soportarse adicionalmente bajo demanda

Canales soportados

- ▶ HTTP/HTTPS

Protocolos soportados

- ▶ Burlap
- ▶ Hessian
- ▶ HTTP invoker
- ▶ JMS



Kinamik Data Integrity
 Diputació 238, àtic 5
 08007 Barcelona España
 Tel: (+34) 931 835 814
 Fax: (+ 34) 934 517 628
www.kinamik.com
 info@kinamik.com