

¿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?

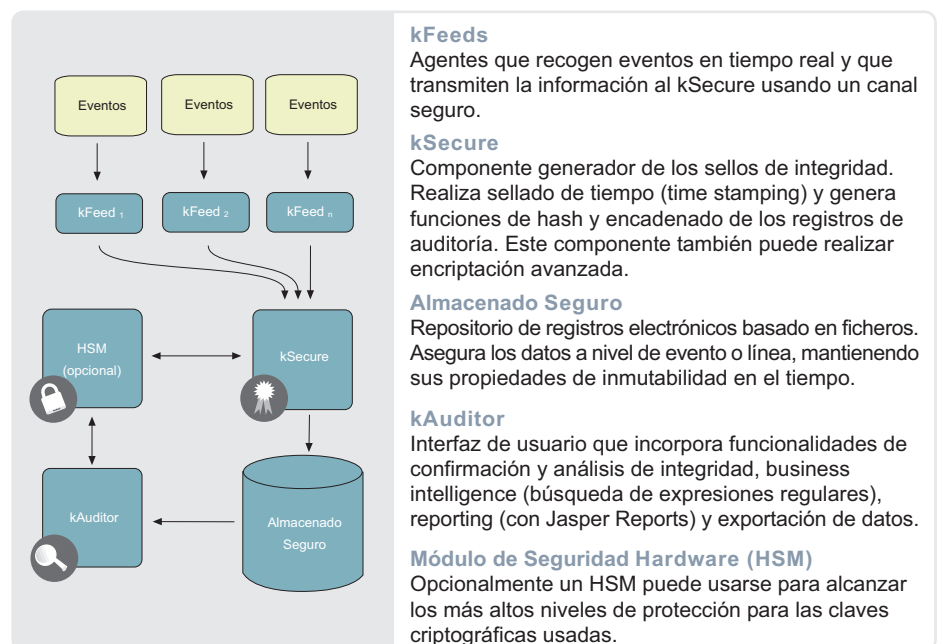
- ▶ Reduce costes asociados a procesos de gobernabilidad, gestión de riesgos y cumplimiento de normativas (GRC)
- ▶ Reduce costes asociados a procesos de auditoría, gestión de pruebas electrónicas (e-discovery) y procesos de investigación de informática forense
- ▶ Disuade el fraude y reduce el riesgo 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 o sobrepasa 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, FISMA, Ley 11/2007, etc.)

¿Puede confiar en los registros electrónicos usados como prueba electrónica, o sujetos a leyes y normativas?

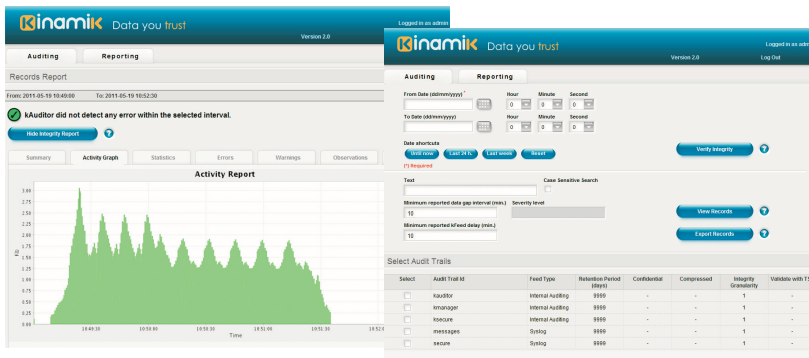
La gestión de la información y riesgos, el cumplimiento de leyes y normativas y el correcto tratamiento de la información en caso de litigios son necesidades prioritarias para las organizaciones. Representan un desafío creciente para las empresas, ya que es cada vez más difícil y costoso cumplir con los mandatos, la amenaza interna aumenta día a día y los requerimientos asociados a la gestión, presentación y aceptación de pruebas electrónicas son cada vez más complejos y costos de seguir - no hacerlo supone grandes riesgos para las organizaciones.

Kinamik Secure Audit Vault hace frente a estos desafíos al construir en tiempo real una bóveda centralizada y segura para la información. La tecnología de Kinamik es capaz de procesar cualquier flujo continuo de datos, incluyendo trazas de auditoría (logs), video y audio digital y ficheros de interceptación legal de telecomunicaciones. Simplifica las tareas de archivo, preservación y búsqueda de información manteniendo los registros en forma segura con los más altos niveles de integridad, y es capaz de manejar sin sobresaltos altos volúmenes de información desde diversas fuentes, incluyendo aplicaciones, bases de datos, servidores y dispositivos conectados a redes. Preserva la información en formato nativo (raw) aplicando un sello de inviolabilidad a nivel de cada evento, permitiendo demostrar en forma fehaciente e irrefutable si algún registro ha sido manipulado.

Kinamik Secure Audit Vault contribuye en la reducción de costes asociados al cumplimiento de leyes, disminuye el riesgo de ataques internos al entregar información irrefutable de las actividades realizadas (incluso por usuarios con privilegios) y soporta procesos judiciales al aumentar el valor probatorio de la información procesada para su uso como evidencia, otorgando pruebas incuestionables de su integridad.



Kinamik Secure Audit Vault · Arquitectura de Producto



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

Funcionalidades destacadas

Seguridad y cumplimiento

- ▶ Encriptación de datos opcional: usando avanzados protocolos estándar los datos pueden ser opcionalmente encriptados para proteger su confidencialidad, con gestión de claves de encriptación independientes para cada auditor.
- ▶ Herramienta para política de retención de datos: permite la definición de políticas independientes para cada fuente de información, cumpliendo con leyes, regulaciones y estándares (PCI-DSS, HIPAA, Basel II, LOPD, Ley 11/2007, SOX, etc.)
- ▶ Informe de integridad de los datos: una sencilla interfaz gráfica permite la evaluación de la integridad de los datos, señalando de forma precisa -a nivel de evento o línea de registro- cualquier alteración o modificación.
- ▶ Gestión de usuario por LDAP: Kinamik Secure Audit Vault se integra con sistemas de gestión de usuarios y es compatible con LDAPv3 y Active Directory.

Business intelligence

- ▶ Fácil integración con herramientas de reporting: exporte los resultados de verificación de la integridad Jasper Reports, creando así reportes personalizados.

Reducción de costes

- ▶ Compresión de mensajes en tránsito: reduce el tráfico en red mediante la compresión de hasta 70% de los mensajes enviados al componente de protección de integridad.
- ▶ Capacidades de compresión para almacenamiento y archivado: la funcionalidad de compresión permite reducción de costes de almacenamiento, alcanzando ratios de compresión de hasta 5:1.
- ▶ Almacenamiento seguro basado en ficheros: reduce drásticamente el costo total de propiedad (TCO) al simplificar la gestión de la información y eliminar la necesidad de licencias y administradores de bases de datos.
- ▶ 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, Inc.

La tecnología de Kinamik protege en tiempo real los registros electrónicos en tránsito o en reposo al evidenciar cualquier intento de manipulación. Creamos una Bóveda de Auditoría Centralizada para los datos sensibles con integridad y autenticidad al más alto nivel de granularidad, creando en el mundo digital niveles de evidencia análogos al de los registros tradicionales basados en papel. Kinamik disuade, detecta y demuestra cualquier manipulación para garantizar la autenticidad e integridad de la información.

Nuestra misión es elevar el nivel de confianza, facilitar la rendición de cuentas y asegurar la privacidad en industrias que trabajen con grandes volúmenes de información sensible y de alto valor. Ofrecemos avanzadas funcionalidades de protección de la integridad en industrias como banca y finanzas, ciencias de la salud, transporte, agencias de sector público y alojamiento de IT.

Kinamik es McAfee SIA Partner y Sun Startup Essential Partner.

Kinamik es una marca de Kinamik Data Integrity, Inc. El resto de marcas incluidas en el documento son propiedad de sus respectivos propietarios.

© 2011, Kinamik Data Integrity, Inc.

Arquitectura

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

Algoritmos criptográficos

- ▶ Encriptación: AES 256
- ▶ Criptografía simétrica: SHA-256
- ▶ Criptografía asimétrica: RSA 1024+
- ▶ La implementación criptográfica puede ser ajustada bajo necesidad, por usuarios autorizados, para seguridad o rendimiento

Plataformas soportadas

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

Fuentes soportadas

- ▶ Mensajes Syslog
- ▶ 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
- ▶ Windows Event Log
- ▶ Conector de monitorización de carpetas para captura automática de ficheros de texto
- ▶ Conector basado en Servicio Web para conectar con aplicaciones de terceras partes
- ▶ Nuevas plataformas están siendo constantemente añadidas, y pueden soportarse adicionalmente bajo demanda

Protocolos soportados

- ▶ HTTP invoker
- ▶ JMS
- ▶ HTTP/HTTPS



Kinamik Data Integrity, Inc.
303 Twin Dolphin Drive
Redwood City, CA 94065, USA
Tel: (+1) 650 632 4408
Fax: (+1) 650 551 9901

Kinamik Data Integrity, S.L.
Diputació 238, àtic 5
08007, Barcelona, Spain
Tel: (+34) 931 835 814
Fax: (+34) 933 041 681

www.kinamik.com
info@kinamik.com