

¿Qué es Kinamik Secure Audit Vault?

Kinamik Secure Audit Vault es una solución software innovadora que recoge, asegura y centraliza la información de auditoría desde diversas fuentes, mientras proporciona la prueba fehaciente de su integridad y la garantía de no repudio. Ayuda a las organizaciones a reducir los costes asociados a procesos de auditoría y cumplimiento normativo, a mitigar la amenaza interna, y a aumentar el valor probatorio en caso de litigio.

¿Qué beneficios se obtienen con Kinamik Secure Audit Vault?

- ▶ Reduce los costes asociados a procesos GRC, gestión de pruebas electrónicas (e-discovery), auditoría y a procesos de investigación de informática forense
- ▶ Apoya en los procesos judiciales al aumentar el valor probatorio de los registros electrónicos y revertir la carga de la prueba
- ▶ Reduce el riesgo de manipulación no deseada o maliciosa, proporcionando confianza de extremo a extremo y garantía de no repudio en destino
- ▶ Se adecúa a las más estrictas reglamentaciones de lucha contra el fraude y mejores prácticas (por ejemplo, SOX, PCI-DSS, NIST, etc.) especialmente en hacer frente a las garantías de la identidad

El gap de seguridad en la Gestión de Identidades (IDAM)

Las soluciones de gestión de identidades y acceso (*IDAM* en inglés) entregan claros beneficios a las organizaciones, incluyendo reducción de costes en IT y soporte técnico (help desk), mejoras en la gestión de la seguridad, aumento en la productividad y simplificación de procesos de cumplimiento de normativas. Sin embargo, la implementación de dichas soluciones no está exenta de riesgos, con elementos clave por lo general no considerados: leyes y normativas requieren registros detallados de las actividades de usuarios como demostración del seguimiento de sus directrices (accesos privilegiados, separación de funciones, etc.). Así, se genera un gap de seguridad importante por la falta de garantías en la asociación entre la aplicación, sistema operativo o base de datos que genera un evento, y la identidad asociada a ese evento.

Para entregar esta necesaria confianza de extremo a extremo, las organizaciones deben ser capaces de proporcionar garantías de la no manipulación de la asociación entre eventos y usuarios. La fiabilidad requerida, al ser de extremo a extremo, va desde la provisión de una identidad y su asociación a una persona o recurso, hasta la correlación que una solución de entrada única (SSO) hará a una aplicación o cualquier otro componente. Estas asociaciones y correlaciones, reflejadas en los registros de auditoría (logs) de cada sistema, son fácilmente modificables por cualquier usuario con los adecuados privilegios de acceso. Como resultado, cualquier punto débil en la cadena de la gestión de identidad puede ocasionar que un usuario dispute su asociación con una identidad y con el evento relacionado. Este hecho puede traer consecuencias catastróficas para una organización en caso de necesidad (litigios, investigaciones forenses, auditorías internas o externas, etc).

Kinamik Secure Audit Vault ayuda a satisfacer los requerimientos de necesidad de confianza de extremo a extremo mediante la captura de los registros de auditoría generados en toda la secuencia de la gestión de identidad.

Profundo impacto en toda la organización

Esta disminución de confianza genera un gran impacto en diversas áreas y procesos:

- ▶ **Cumplimiento de normativas:** la legislación actual exige la presentación de una única identidad para aplicar políticas como segregación de funciones, controles de acceso privilegiados, etc. Las implementaciones no seguras de sistemas IDAM generan faltas de fiabilidad en la asociación de un usuario a un evento auditable, elemento identificado por auditores como conflictivo ante los requisitos de confianza explicitados en leyes y reglamentos (SOX, PCI-DSS, etc).
- ▶ **Legal:** una de las tareas de las organizaciones es autenticar correctamente a los usuarios de los sistemas. Los registros de auditoría, a menudo usados como prueba, se enfrentan a un escrutinio creciente y su autenticidad es cada vez más cuestionada. Si la asociación usuario-registro de auditoría ve debilitado su valor probatorio, los equipos jurídicos se enfrentan a una difícil tarea, gestionando el posible impacto de un fallo judicial.
- ▶ **Seguridad:** una robusta asociación entre un evento y un usuario permite la correcta ejecución y monitorización de la implementación de políticas de seguridad. No poder entregar pruebas fidedignas de la asociación de un usuario a un registro de auditoría pone en riesgo las mismas bases de seguridad de la organización.
- ▶ **TIC:** permitir la confianza en los registros de auditoría generados por un usuario (y su asociación a los repositorios de identidad) es un atributo fundamental para lograr razonable seguridad en los sistemas TIC y para apoyar el cumplimiento de requerimientos legales en lo que respecta a la obtención de confianza de extremo a extremo. El aumento en la complejidad de los servicios TIC y a la creciente adopción de Cloud Computing ha aumentado enormemente la importancia de este punto.

► **Línea de Negocio:** cada unidad de negocio es el último responsable y titular de sus datos (generados y utilizados). La falta de garantías en la identidad electrónica y en la confianza de extremo a extremo pueden tener graves consecuencias en la línea de negocio.

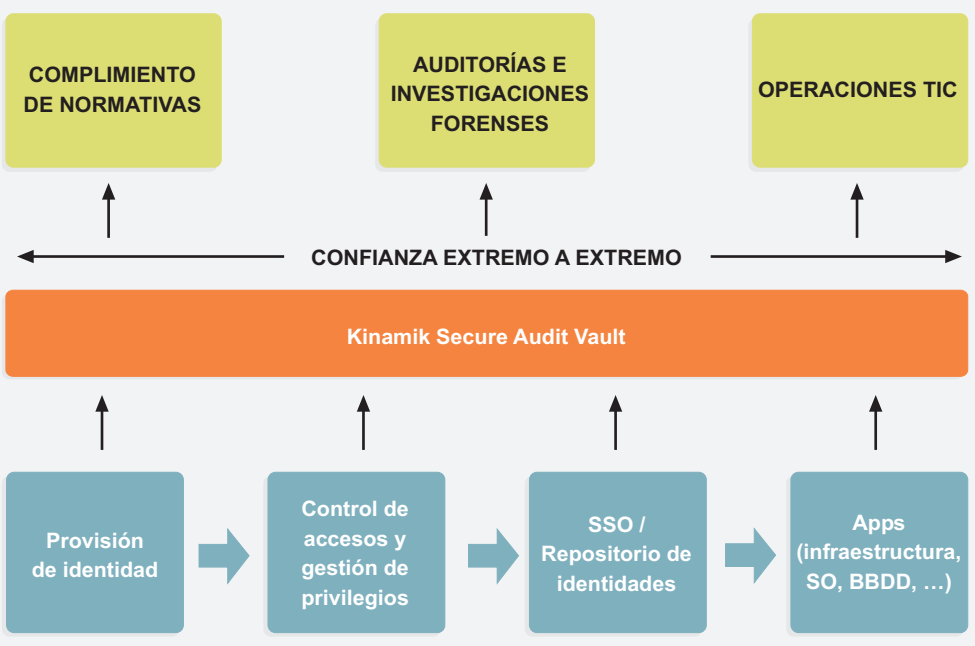
¿Cómo ayuda Kinamik Secure Audit Vault?

Los agentes recolectores de datos del Kinamik Secure Audit Vault (kSAV) capturan y transmiten en tiempo real los eventos de los registros de auditoría, al momento en que son generados. Usando un canal seguro encriptado los eventos son transmitidos hasta el módulo de procesamiento de la integridad, tras lo cual cualquier intento de manipulación en los eventos queda evidenciado. Al implementar Kinamik Secure Audit Vault como soporte de los componentes de una solución IDAM y de los dispositivos o aplicaciones del sistema, se entregan garantías de extremo a extremo de la integridad y autenticidad de los registros de auditoría y, más importante aún, confianza en la asociación usuario-evento.

Pueden lograrse mayores niveles de seguridad con el uso complementario de:

- un módulo de seguridad hardware (HSM) para proteger las llaves criptográficas;
- una Autoridad de Sellado de Tiempo (TSA) que actúe como tercero de confianza;
- la activación de la opción de cifrado de datos del kSAV, dotando a los datos de la propiedad de confidencialidad.

El modelo de tarificación de Kinamik, basado en el máximo de datos procesados diariamente, permite el despliegue de tantos conectores e instalaciones como sea necesario (balanceo de carga, alta disponibilidad, tolerancia a fallos, etc). Cada servidor de kSAV es capaz de procesar hasta 40.000 eventos/segundo. Además, la funcionalidad de control de acceso de kSAV permite que los usuarios accedan sólo a la información a la que están autorizados.



Kinamik Secure Audit Vault entrega confianza extremo a extremo, soportando procesos de cumplimiento de normativas, operaciones TIC y procesos de auditoría e investigación.



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 McAfee SIA Partner y Sun Startup Essential 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.

Funcionalidades seleccionadas

► **Compresión de mensajes en tránsito:** reduce el tráfico en red mediante la compresión de hasta el 70% de los mensajes enviados al componente de protección de integridad.

► **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.

► **Herramienta para política de retención de datos:** permite la definición de políticas de retención de datos independientes para cada fuente de información, cumpliendo con mandatos específicos de diversas leyes, regulaciones y estándares (PCI-DSS, HIPAA, Basel II, LOPD, Ley 11/2007, SOX, MiFID, etc).

► **Búsqueda de expresiones regulares:** Kinamik Secure Audit Vault ofrece funcionalidades de búsqueda de expresiones regulares y cadenas de texto en los datos securizados.

► **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.

► **Capacidades de compresión para almacenamiento y archivo:** la funcionalidad de compresión del Kinamik Secure Audit Vault permite reducción de costes de almacenamiento, 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.



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