

Què és Kinamik Secure Audit Vault?

Kinamik Secure Audit Vault és una solució software innovadora que recull, assegura i centralitza la informació d'auditoria des de diverses fonts, mentre proporciona la prova fefaent de la seva integritat i la garantia de no repudi. Ajuda a les organitzacions a reduir els costos associats a processos d'auditoria i compliment normatiu, a mitigar l'amenaça interna, i a augmentar el valor probatori en cas de litigi.

Quins beneficis s'obtenen en utilitzar Kinamik Secure Audit Vault?

- ▶ Redueix els costos associats als processos GRC, gestió de proves electròniques (e-discovery), auditoria i processos d'investigació d'informàtica forense
- ▶ Recolza en els processos judicials en augmentar el valor probatori dels registres electrònics i revertir la càrrega de la prova
- ▶ Redueix el risc de manipulació no desitjada o maliciosa, proporcionant confiança d'extrem a extrem i garantia de no repudi en destí
- ▶ S'adequa a les més estrictes reglamentacions de lluita contra el frau i millors pràctiques (per exemple, SOX, PCI-DSS, NIST, etc.) especialment en fer front a les garanties de la identitat

El gap de seguretat en la Gestió d'Identitats (IdAM)

Les solucions de gestió i accés d'identitats (IdAM en anglès) lliuren clars beneficis a les organitzacions, incloent reducció de costos en IT i suport tècnic (help desk), millores en la gestió de la seguretat, augment en la productivitat i simplificació dels processos de compliment de normatives. Tanmateix, la implementació de les esmentades solucions no és exempta de riscos, amb elements clau en general no considerats: les lleis i normatives requereixen registres detallats de les activitats d'usuaris com a demostració del seguiment de les seves directrius (accessos privilegiats, separació de funcions, etc.). Així, es genera un gap de seguretat important per la falta de garanties en l'associació entre l'aplicació, sistema operatiu o base de dades que genera un esdeveniment, i la identitat associada a aquest esdeveniment.

Per lliurar aquesta confiança necessària d'extrem a extrem, les organitzacions han de ser capaces de proporcionar garanties de la no manipulació de l'associació entre esdeveniments i usuaris. La fiabilitat requerida, al ser d'extrem a extrem, va des de la provisió d'una identitat i la seva associació a una persona o recurs, fins a la correlació que una solució d'entrada única (SSO) farà a una aplicació o qualsevol altre component. Aquestes associacions i correlacions, reflectides en els registres d'auditoria (logs) de cada sistema, són fàcilment modificables per qualsevol usuari amb els adequats privilegis d'accés. Com a resultat, qualsevol punt feble a la cadena de la gestió d'identitat pot ocasionar que un usuari disputi la seva associació amb una identitat i amb l'esdeveniment relacionat. Aquest fet pot portar conseqüències catastròfiques per a una organització en cas de necessitat (litigis, investigacions forenses, auditories internes o externes, etc).

Kinamik Secure Audit Vault ajuda a satisfer els requeriments de necessitat de confiança d'extrem a extrem mitjançant la captura dels registres d'auditoria generats en tota la seqüència de la gestió d'identitat.

Gran impacte en tota l'organització

Aquesta falta de confiança genera un gran impacte en diverses àrees i processos:

- ▶ *Compliment de normatives*: la legislació actual exigeix la presentació d'una única identitat per aplicar polítiques com la segregació de funcions, controls d'accés privilegiats, etc. Les implementacions no segures de sistemes IdAM generen faltes de fiabilitat en l'associació d'un usuari a un esdeveniment auditable, element identificat per auditors com a conflictiu davant dels requisits de confiança explicitats en lleis i reglaments (SOX, PCI-DSS, etc).
- ▶ *Legal*: una de les tasques que qualsevol organització té és la d'autenticar correctament els usuaris dels sistemes. Els registres d'auditoria, sovint utilitzats com a prova, s'enfronten a un major escrutini i la seva autenticitat és cada vegada més qüestionada. Si l'associació usuari-registre d'auditoria veu debilitat el seu valor probatori, els equips jurídics s'enfronten a una difícil tasca, gestionant el possible impacte d'un error judicial.
- ▶ *Seguretat*: una robusta associació entre un esdeveniment i un usuari permet la correcta execució i monitoratge de la implementació de polítiques de seguretat. No poder lliurar proves fidedignes de l'associació d'un usuari a un registre d'auditoria posa en risc les mateixes bases de seguretat de l'organització.
- ▶ *TIC*: permetre la confiança dels registres d'auditoria generats per un usuari (i la seva associació als dipòsits d'identitat) és un atribut fonamental per aconseguir una seguretat raonable en els sistemes TIC i recolzar el compliment dels requisits legals d'un sistema extrem a extrem de confiança. L'augment de la complexitat dels serveis TIC i la creixent adopció del Cloud Computing ha augmentat enormement la importància d'aquesta qüestió.

► **Línia de Negoci:** cada unitat de negoci és l'últim responsable i el titular de les seves dades (generats i utilitzats). La falta d'assegurament de la identitat i la confiança extrem a extrem poden tenir greus conseqüències en la línia de negoci.

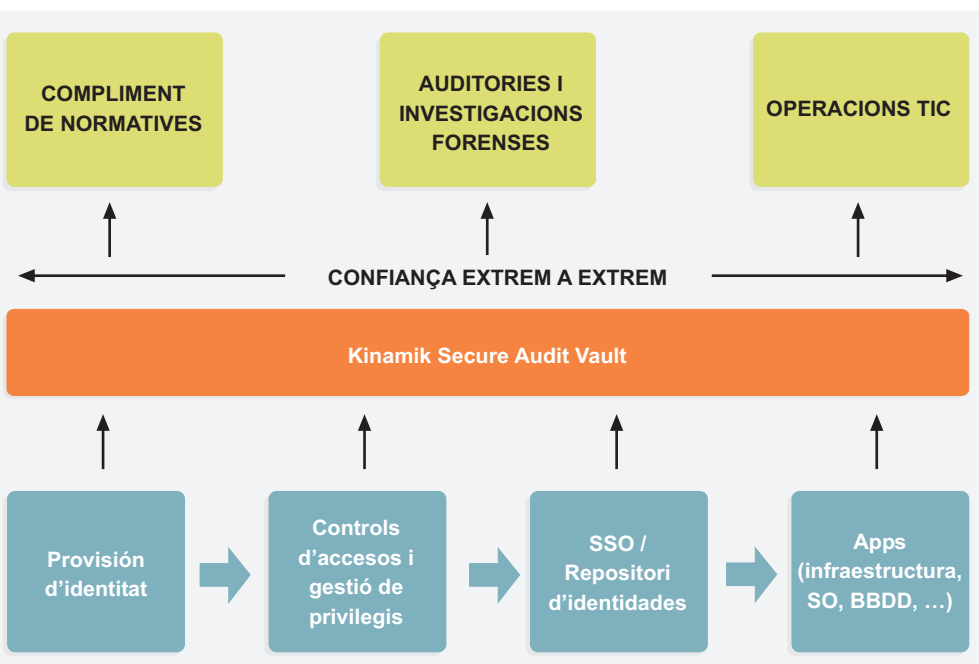
Com ajuda el Kinamik Secure Audit Vault?

Els agents recol·lectors de dades del Kinamik Secure Audit Vault (kSAV) capturen i transmeten en temps real els esdeveniments dels registres d'auditoria, al moment en què són generats. Usant un canal segur encriptat els esdeveniments són transmesos fins al mòdul de processament de la integritat, després del qual qualsevol intent de manipulació en els esdeveniments queda evidenciat. En implementar Kinamik Secure Audit Vault com a suport dels components d'una solució IdAM i dels dispositius o aplicacions del sistema, es lliuren garanties d'extrem a extrem de la integritat i autenticitat dels registres d'auditoria i, més important encara, confiança en l'associació usuari-esdeveniment.

Poden aconseguir-se majors nivells de seguretat amb l'ús complementari de:

- un mòdul de seguretat opcional (HSM) per protegir les claus criptogràfiques;
- una Autoritat de Segellament de Temps (TSA) que actui com a tercer de confiança;
- l'activació de l'opció de xifrat de dades del kSAV, dotant a les dades de la propietat de confidencialitat.

El model de tarifació de Kinamik, basat en el màxim de dades processades diàriament, permet el desplegament de tants connectors i instal·lacions com sigui necessari (balanceig de càrrega, alta disponibilitat, tolerància a errors, etc.). Cada servidor de kSAV és capaç de processar fins 40.000 esdeveniments/segon. A més, la funcionalitat de control d'accés de kSAV permet que els usuaris accedeixin només a la informació a què estan autoritzats.



Kinamik Secure Audit Vault lliura confiança extrem a extrem, recolzant processos de compliment de normatives, operacions TIC i processos d'auditoria i investigació.

Sobre Kinamik Data Integrity

El software de Kinamik Data Integrity protegeix la manipulació dels registres digitals. Construïm una volta d'auditoria centralitzada per a registres sensibles d'auditoria amb integritat i autenticitat al nivell de granularitat més alt possible, creant un nivell d'evidència al món digital similar al dels registres tradicionals basats en paper. Kinamik dissuadeix, detecta i demostra qualsevol intent de manipulació per garantir que la informació digital sigui correcta.

La nostra missió és elevar el nivell de confiança en les organitzacions, facilitar la rendició de comptes i assegurar la privacitat en indústries que treballin amb grans volums d'informació sensible.

Kinamik és McAfee SIA Partner i Sun Startup Essential Partner.



S'han realitzat tots els esforços possibles per assegurar que la informació inclosa en aquest document és precisa i està actualitzada en el moment de ser publicada. No obstant això, els productes descrits aquí estan sotmesos a un continu desenvolupament i millora i Kinamik es reserva el dret de modificar les especificacions en qualsevol moment. Declinem tota responsabilitat cap a aquest document, i no hi ha cap obligació contractual ni directa ni indirectament amb el seu contingut. Kinamik és una marca de Kinamik Data Integrity, S.L. La resta de marques incloses al document són propietat dels seus respectius propietaris.

© 2010, Kinamik Data Integrity S.L.

Funcionalidades seleccionadas

► **Compresió de missatges en trànsit:** redueix el tràfic en xarxa mitjançant la compresió de fins i tot el 70% en la mida dels missatges enviats al component de segellat digital per a la protecció de la integritat.

► **Gestió d'usuari per LDAP:** Kinamik Secure Audit Vault s'integra amb els sistemes de gestió d'usuaris i és compatible amb LDAP i Active Directory.

► **Eina de política de retenció de dades:** defineixi en forma independent diferents polítiques de retenció per a cada font d'informació, complint així amb els períodes específics de retenció exigits per diverses lleis, regulacions i estàndards (per ej. PCI-DSS, HIPAA, Basel II, SOX, MiFID, etc).

► **Recerca expressions regulars:** utilitzi les capacitats de recerca del Kinamik Secure Audit Vault per localitzar de forma precisa i exacta cadenes de text i expressions en les dades securitzades.

► **Informe d'integritat de les dades:** una senzilla interfície gràfica permet l'avaluació de la integritat de les dades, assenyalant en forma precisa -a nivell d'esdeveniment o línia de registre- qualsevol alteració o modificació.

► **Capacitats de compresió per a emmagatzemament i arxivat:** redueixi costos d'emmagatzemament i arxivat d'informació usant les funcionalitats de compresió del Kinamik Secure Audit Vault, assolint proporcions de compresió de fins i tot 5:1.

► **Fàcil integració amb eines de reporting:** exporti fàcilment els resultats de verificació de la integritat i desenvolupi informes personalitzats usant Jasper Reports.

Kinamik
Data you trust

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